

Exhibit 5

IN THE UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF TEXAS
SHERMAN DIVISION

THE TRANSPARENCY PROJECT,	§	
	§	
Plaintiff,	§	CIVIL ACTION No. 4:20CV467
	§	
v.	§	
	§	
U.S. DEPARTMENT OF JUSTICE, et al.,	§	JUDGE SEAN D. JORDAN
	§	
Defendants.	§	

DECLARATION OF KIRK WIEBE

My name is Kirk Wiebe, I am greater than 18 years of age, I am competent to testify, and I hereby testify as follows under penalty of perjury under the laws of the United States, as witnessed by my signature below:

1. I served in the U.S. Air Force Security Service from 1964 until 1967. After my military service, I spent 22 years working at the National Security Agency (the "NSA"). The NSA is the signals intelligence agency within the Department of Defense, and I worked in a variety of analytical roles that required familiarity with intelligence analysis and cutting-edge surveillance technology.
2. Since leaving the NSA, I have remained familiar with basic and advanced information technology capabilities in the public and private sector.
3. It is common knowledge that private individuals and companies possess the capability of inserting "fingerprints" into documents for purposes of "false flag" operations. Specifically, an agency or individual can easily alter an email to make it appear that individuals from another country, *e.g.*, Russia or China, were responsible for "hacking" that email when, in reality, the email was not hacked at all. In such a false flag operation, the objective is to shift blame to a third party.
4. The foregoing capability has existed for decades, and its availability is widely known. Consider, for example, the following excerpt from *Wired* magazine:

The difficulty of proving the source of an attack—the so-called attribution problem—has plagued cybersecurity since practically the dawn of the internet. Sophisticated hackers can route their connections through

circuitous proxies and blind alleys, making it almost impossible to follow their tracks. Forensic analysts have nonetheless learned how to determine hackers' identities by other means, tying together clues in code, infrastructure connections, and political motivations.

In the past few years, however, state-sponsored cyberspies and saboteurs have increasingly experimented with another trick: planting false flags. Those evolving acts of deception, designed to throw off both security analysts and the public, have given rise to fraudulent narratives about hackers' identities that are difficult to dispel, even after governments announce the official findings of their intelligence agencies. It doesn't help that those official findings often arrive weeks or months later, with the most convincing evidence redacted to preserve secret investigative techniques and sources.

Andy Greenberg, “The Untold Story of the 2018 Olympics Cyberattack, the Most Deceptive Hack in History,” October 17, 2019 *Wired*, (<https://www.wired.com/story/untold-story-2018-olympics-destroyer-cyberattack/>) (attached as Internal Exhibit A); *see also* Josh Fruhlinger, “What is a false flag? How state-based hackers cover their tracks,” January 9, 2020 CSO (<https://www.csoonline.com/article/3512027/what-is-a-false-flag-how-state-based-hackers-cover-their-tracks.html>); and Patrick Howell O’Neill, “Chinese hackers disguised themselves as Iran to target Israel,” August 10, 2021 *MIT Technology Review* (<https://www.technologyreview.com/2021/08/10/1031622/chinese-hackers-false-flag-iran-israel-fireeye/>).

5. If the USG were to deny having such capabilities, that would be on par with denying that it uses mobile phones or word processing software. Furthermore, the USG has already admitted that the Central Intelligence Agency (“CIA”) possesses such capabilities.
6. On March 7, 2017, Wikileaks published “Vault 7,” which contained thousands of records and millions of lines of code about the CIA’s hacking capabilities. *See* March 7, 2017 Press Release, Wikileaks (<https://wikileaks.org/ciav7p1/>) (attached as Internal Exhibit B). That press release includes the following paragraphs:

The CIA's Remote Devices Branch's UMBRAGE group collects and maintains a substantial library of attack techniques 'stolen' from malware produced in other states including the Russian Federation.

With UMBRAGE and related projects the CIA cannot only increase its total number of attack types but also misdirect attribution by leaving behind the "fingerprints" of the groups that the attack techniques were stolen from.

UMBAGE components cover keyloggers, password collection, webcam capture, data destruction, persistence, privilege escalation, stealth, anti-virus (PSP) avoidance and survey techniques.

Id. I have reviewed “Vault 7” and concluded that the foregoing statement is correct. Specifically, the CIA possessed the technical capability in 2017 to insert Russian “fingerprints” into emails such as those that were purportedly “hacked” from the DNC in 2016. Notably, the USG verified that the contents of “Vault 7” were indeed authentic CIA records / files when it filed criminal charges against a Joshua Schulte, a former CIA employee. *See U.S. v. Joshua Adam Schulte*, 436 F.Supp.3d 698, 702 (S.D.N.Y. 2020).

7. In my professional opinion, there is no national security reason to deny that the USG possesses the capability to insert “fingerprints” (*e.g.*, language, code, or other markers) into documents or communications for purposes of shifting blame to other parties, whether foreign or domestic.
8. Based on my familiarity with social media systems and internet technologies, I attest that it would not be difficult to create an account on Twitter (or other social media) and make it appear that the account was created by another person, entity, or government. It is quite easy, for example, to utilize an overseas server (*e.g.*, via a virtual private network) to make it appear that web traffic originated in another country.
9. The United States government has previously created false accounts on social media for purposes of distributing propaganda. *See* Brady Knox, “Twitter and Meta take down pro-U.S. propaganda campaign targeting Middle East,” August 26, 2022 *Washington Examiner* (<https://www.msn.com/en-us/news/world/twitter-and-meta-take-down-pro-u-s-propaganda-campaign-targeting-middle-east/ar-AA1191y6>) (attached as Internal Exhibit C).
10. I do not know whether the USG created “Guccifer 2.0” or “DCLeaks” on Twitter, but such a capability would be unremarkable insofar as it already exists in the private sector. In my professional opinion, there could be no national security reason to deny that the USG possesses such capabilities. If nothing else, the USG could hire a high school student on the open market to achieve such a result.

11. In response to news that national security reporter James Gordon Meek had been arrested on charges of transporting child pornography, *see, e.g.*, Ben Feuerherd and Olivia Land, “Ex-ABC News reporter James Gordon Meek hit with child pornography charge,” February 1, 2023 *New York Post* (<https://nypost.com/2023/02/01/reporter-james-gordon-meek-charged-in-child-pornography-case/>), Mr. Clevenger separately requested my opinion about whether the USG possesses the capability of inserting fabricated evidence onto the computers or other electronic devices of unwitting third parties.
12. I do not know whether the USG inserted child pornography onto Mr. Meek’s laptop, but there are multiple avenues for inserting fabricated evidence onto someone’s electronic devices. Obviously, one might surreptitiously take custody of an electronic device such as a laptop computer, then utilize that device to “surf” the internet and download images of child pornography before returning that device to its owner. One might do the same by uploading files from a thumb drive or other portable drive. One might also insert files via routine hacking.
13. Sophisticated hackers – including solo hackers or hackers in the private sector – can remotely gain access to an electronic device and then insert malicious files of almost any kind, including child pornography. In the report of Special Counsel Robert M. Mueller, for example, he and the FBI concluded that Russian hackers were able to gain access to the Democratic National Committee’s computer servers, download emails from those servers, and then transfer the emails to Wikileaks for publication in 2016.
14. It is widely known and completely unremarkable that sophisticated hackers can insert malicious files and then “cover their tracks,” *i.e.*, by hiding any evidence that they hacked into an electronic device and inserted the malicious files. The Catholic News Service recently reported that an activist priest was imprisoned by India based on false evidence that had been planted on his computer by hackers. *See* “Hackers planted false files implicating Indian Jesuit Father Swamy who died in prison,” December 15, 2022, *America: The Jesuit Review* (<https://www.americamagazine.org/faith/2022/12/15/hackers-planted-false-files-implicating-indian-jesuit-died-prison-244351>) (attached as Internal Exhibit D). The priest died before an American firm was able to prove that the files had been inserted by third parties. *Id.*
15. In 2009, the Associated Press reported that innocent people had been imprisoned because viruses inserted child pornography files on their computers. *See* “Viruses Frame PC Owners for Child Porn,” November 9, 2009 *Associated Press* (<https://www.cbsnews.com/news/viruses-frame-pc-owners-for-child-porn/>) (attached as Internal Exhibit E). One might also

deceive an innocent person into unwittingly downloading child pornography, by means of “clickjacking.” *See, e.g.*, <https://www.imperva.com/learn/application-security/clickjacking/> (attached as Internal Exhibit F, explaining the clickjacking phenomenon). Somewhat relatedly, a federal judge dismissed child pornography charges in 2016 after the FBI refused to disclose the hacking methodology that it used to track the defendant online. *See* Laura Hautala, “FBI won’t reveal hack, so child porn evidence tossed,” May 25, 2016 CNET (<https://www.cnet.com/tech/services-and-software/fbi-wont-reveal-hack-so-child-porn-evidence-tossed/>) (attached as Internal Exhibit G).

16. Furthermore, Vault 7 revealed that as of 2017, the CIA possessed very sophisticated tools for hacking into electronic devices and inserting files, malware and fabricated evidence.
17. In my professional opinion, there could be no national security reason for the USG to deny that it possesses the ability to insert files (whether child pornography or any other content), particularly because Vault 7 is now public and because those capabilities are readily accessible in the private sector. One could, for example, secretly hire a sophisticated hacker without ever meeting him or her (*e.g.*, via the dark web) and then pay him or her via an offshore account or with digital currency.
18. Again, I do not know whether anyone planted false evidence on Mr. Meek’s computer, but there is no national security reason to deny that such capabilities are in existence. If the USG denied that it had *access* to those capabilities, it would be on par with denying that it had access to mobile phones and word processing software.
19. It is widely known that hackers in the private sector possess the capability to insert monitoring software on electronic devices, *e.g.*, to monitor the keystrokes, conversations, or electronic communications of the owner or user of the device. *See, e.g.*, Nikolay Grebennikov, March 29, 2007 SecureList (<https://securelist.com/keyloggers-how-they-work-and-how-to-detect-them-part-1/36138/>) (attached as Internal Exhibit H). Vault 7 reveals that the CIA possessed this capability as of 2017. In my professional opinion, there could be no national security reason for the USG to deny that it possesses such capabilities.

THE DECLARANT SAYS NOTHING FURTHER.

March 16, 2023


Kirk Wiebe

Internal Exhibit A

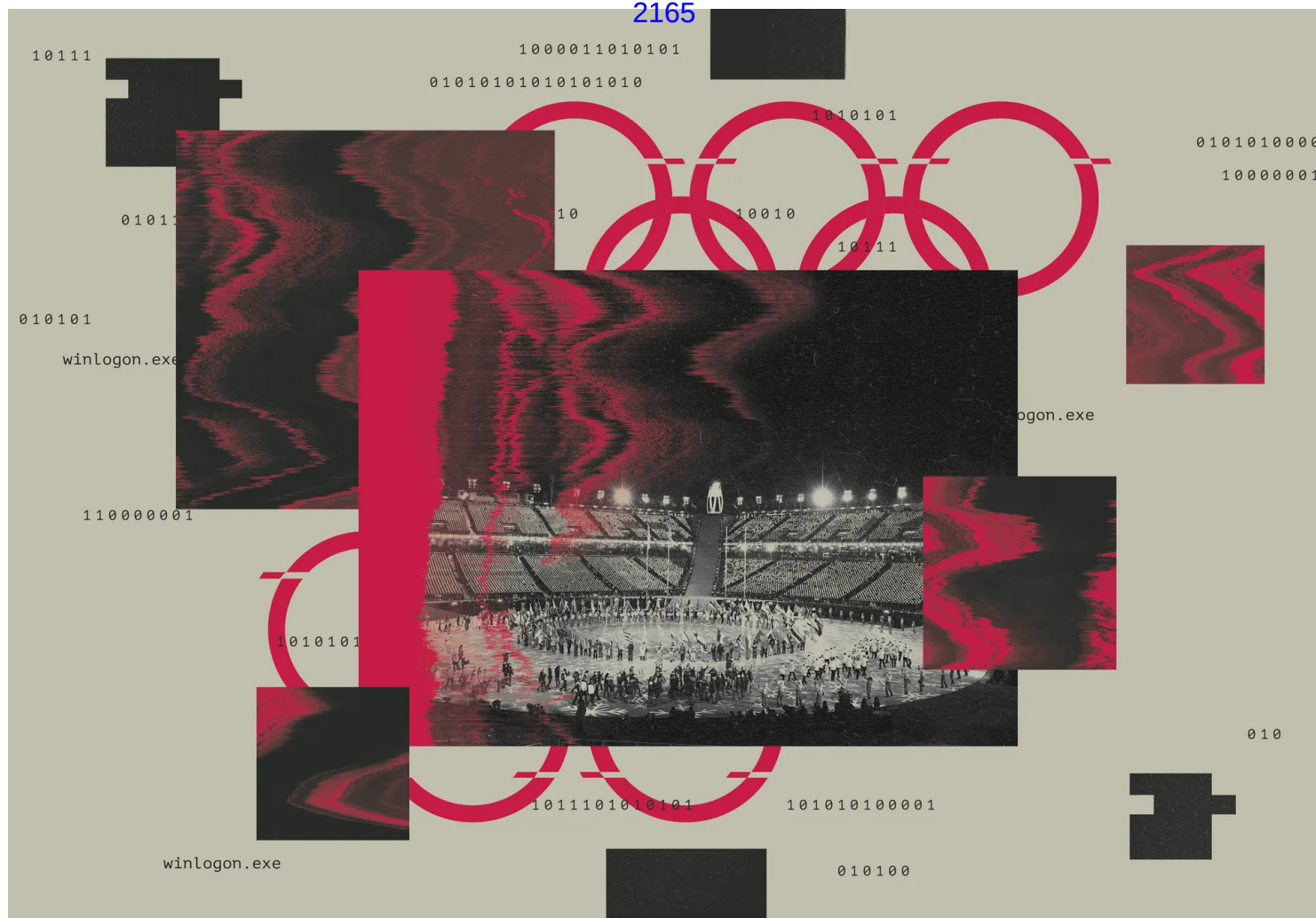


ILLUSTRATION: JOAN WONG

ANDY GREENBERG EXCERPT SECURITY OCT 17, 2019 6:00 AM

The Untold Story of the 2018 Olympics Cyberattack, the Most Deceptive Hack in History

How digital detectives unraveled the mystery of Olympic Destroyer—and why the next big attack will be even harder to crack.

JUST BEFORE 8 pm on February 9, 2018, high in the northeastern mountains of South Korea, Sang-jin Oh was sitting on a plastic chair a few dozen rows up from the floor of Pyeongchang's vast, pentagonal Olympic Stadium. He wore a gray and red official Olympics jacket that kept him warm despite the near-freezing weather, and

his seat, behind the press section, had a clear view of the raised, circular stage a few hundred feet in front of him. The 2018 Winter Olympics opening ceremony was about to start.

As the lights darkened around the roofless structure, anticipation buzzed through the 35,000-person crowd, the glow of their phone screens floating like fireflies around the stadium. Few felt that anticipation more intensely than Oh. For more than three years, the 47-year-old civil servant had been director of technology for the Pyeongchang Olympics organizing committee. He'd overseen the setup of an IT infrastructure for the games comprising more than 10,000 PCs, more than 20,000 mobile devices, 6,300 Wi-Fi routers, and 300 servers in two Seoul data centers.

That immense collection of machines seemed to be functioning perfectly—almost. Half an hour earlier, he'd gotten word about a nagging technical issue. The source of that problem was a contractor, an IT firm from which the Olympics were renting another hundred servers. The contractor's glitches had been a long-term headache. Oh's response had been annoyance: Even now, with the entire world watching, the company was still working out its bugs?

SANDWORM

A NEW ERA OF CYBERWAR
AND THE HUNT FOR THE KREMLIN'S
MOST DANGEROUS HACKERS

ANDY GREENBERG



team believed the issues with the contractor were manageable. He didn't yet know that they were already preventing some attendees from printing tickets that would let them enter the stadium. So he'd settled into his seat, ready to watch a highlight of his career unfold.

Ten seconds before 8 pm, numbers began to form, one by one, in projected light around the stage, as a choir of children's voices counted down in Korean to the start of the event:

“Sip! ... Gu! ... Pal! ... Chil!”

In the middle of the countdown, Oh's Samsung Galaxy Note8 phone abruptly lit up. He looked down to see a message from a subordinate on KakaoTalk, a popular Korean messaging app. The message shared perhaps the worst possible news Oh could have received at that exact moment: Something was shutting down every domain controller in the Seoul data centers, the servers that formed the backbone of the Olympics' IT infrastructure.

As the opening ceremony got underway, thousands of fireworks exploded around the stadium on cue, and dozens of massive puppets and Korean dancers entered the stage. Oh saw none of it. He was texting furiously with his staff as they watched their entire IT setup go dark. He quickly realized that what the partner company had reported wasn't a mere glitch. It had been the first sign of an unfolding attack. He needed to get to his technology operations center.

As Oh made his way out of the press section toward the exit, reporters around him had already begun complaining that the Wi-Fi seemed to have suddenly stopped working. Thousands of internet-linked TVs showing the ceremony around the stadium and in 12 other Olympic facilities had gone black. Every RFID-based security gate leading into every Olympic building was down. The Olympics' official app, including its digital ticketing function, was broken too; when it reached out for data from backend servers, they suddenly had none to offer.

The Pyeongchang organizing committee had prepared for this: Its cybersecurity advisory group had met 20 times since 2015. They'd conducted drills as early as the

summer of the previous year, simulating disasters like cyberattacks, fires, and earthquakes. But now that one of those nightmare scenarios was playing out in reality, the feeling, for Oh, was both infuriating and surreal. “It's actually happened,” Oh thought, as if to shake himself out of the sense that it was all a bad dream.

Once Oh had made his way through the crowd, he ran to the stadium's exit, out into the cold night air, and across the parking lot, now joined by two other IT staffers. They jumped into a Hyundai SUV and began the 45-minute drive east, down through the mountains to the coastal city of Gangneung, where the Olympics' technology operations center was located.

From the car, Oh called staffers at the stadium and told them to start distributing Wi-Fi hot spots to reporters and to tell security to check badges manually, because all RFID systems were down. But that was the least of their worries. Oh knew that in just over two hours the opening ceremony would end, and tens of thousands of athletes, visiting dignitaries, and spectators would find that they had no Wi-Fi connections and no access to the Olympics app, full of schedules, hotel information, and maps. The result would be a humiliating confusion. If they couldn't recover the servers by the next morning, the entire IT backend of the organizing committee—responsible for everything from meals to hotel reservations to event ticketing—would remain offline as the actual games got underway. And a kind of technological fiasco that had never before struck the Olympics would unfold in one of the world's most wired countries.

Oh arrived at the technology operations center in Gangneung by 9 pm, halfway into the opening ceremony. The center consisted of a large open room with desks and computers for 150 staffers; one wall was covered with screens. When he walked in, many of those staffers were standing, clumped together, anxiously discussing how to respond to the attack—a problem compounded by the fact that they'd been locked out of many of their own basic services, like email and messaging.

All nine of the Olympic staff's domain controllers, the powerful machines that governed which employee could access which computers in the network, had somehow been paralyzed, crippling the entire system. The staff decided on a

temporary workaround: They set all the surviving servers that powered some basic services, such as Wi-Fi and the internet-linked TVs, to bypass the dead gatekeeper machines. By doing so, they managed to bring those bare-minimum systems back online just minutes before the end of the ceremony.

Over the next two hours, as they attempted to rebuild the domain controllers to re-create a more long-term, secure network, the engineers would find again and again that the servers had been crippled. Some malicious presence in their systems remained, disrupting the machines faster than they could be rebuilt.

Oh and his staff worked frantically to rebuild the Olympics' digital nervous system.

A few minutes before midnight, Oh and his administrators reluctantly decided on a desperate measure: They would cut off their entire network from the internet in an attempt to isolate it from the saboteurs who they figured must still have maintained a presence inside. That meant taking down every service—even the Olympics' public website—while they worked to root out whatever malware infection was tearing apart their machines from within.

For the rest of the night, Oh and his staff worked frantically to rebuild the Olympics' digital nervous system. By 5 am, a Korean security contractor, AhnLab, had managed to create an antivirus signature that could help Oh's staff vaccinate the network's thousands of PCs and servers against the mysterious malware that had infected them, a malicious file that Oh says was named simply winlogon.exe.

At 6:30 am, the Olympics' administrators reset staffers' passwords in hopes of locking out whatever means of access the hackers might have stolen. Just before 8 that morning, almost exactly 12 hours after the cyberattack on the Olympics had begun, Oh and his sleepless staffers finished reconstructing their servers from backups and began restarting every service.

Amazingly, it worked. The day's skating and ski jumping events went off with little more than a few Wi-Fi hiccups. R2-D2-style robots pattered around Olympic venues, vacuuming floors, delivering water bottles, and projecting weather reports. A *Boston Globe* reporter later called the games “impeccably organized.” One *USA Today* columnist wrote that “it's possible no Olympic Games have ever had so many

moving pieces all run on time.” Thousands of athletes and millions of spectators remained blissfully unaware that the Olympics' staff had spent its first night fighting off an invisible enemy that threatened to throw the entire event into chaos.

Within hours of the attack, rumors began to trickle out into the cybersecurity community about the glitches that had marred the Olympics' website, Wi-Fi, and apps during the opening ceremony. Two days after the ceremony, the Pyeongchang organizing committee confirmed that it had indeed been the target of a cyberattack. But it refused to comment on who might have been behind it. Oh, who led the committee's response, has declined to discuss any possible source of the attack with WIRED.

The incident immediately became an international whodunit: Who would dare to hack the Olympics? The Pyeongchang cyberattack would turn out to be perhaps the most deceptive hacking operation in history, using the most sophisticated means ever seen to confound the forensic analysts searching for its culprit.

The difficulty of proving the source of an attack—the so-called attribution problem—has plagued cybersecurity since practically the dawn of the internet. Sophisticated hackers can route their connections through circuitous proxies and blind alleys, making it almost impossible to follow their tracks. Forensic analysts have nonetheless learned how to determine hackers' identities by other means, tying together clues in code, infrastructure connections, and political motivations.

In the past few years, however, state-sponsored cyberspies and saboteurs have increasingly experimented with another trick: planting false flags. Those evolving acts of deception, designed to throw off both security analysts and the public, have given rise to fraudulent narratives about hackers' identities that are difficult to dispel, even after governments announce the official findings of their intelligence agencies. It doesn't help that those official findings often arrive weeks or months later, with the most convincing evidence redacted to preserve secret investigative techniques and sources.

When North Korean hackers breached Sony Pictures in 2014 to prevent the release of the Kim Jong-un assassination comedy *The Interview*, for instance, they invented a hacktivist group called Guardians of Peace and tried to throw off investigators

with a vague demand for “monetary compensation.” Even after the FBI officially named North Korea as the culprit and the White House imposed new sanctions against the Kim regime as punishment, several security firms continued to argue that the attack must have been an inside job, a story picked up by numerous news outlets—including WIRED.

When state-sponsored Russian hackers stole and leaked emails from the Democratic National Committee and Hillary Clinton's campaign in 2016, we now know that the Kremlin likewise created diversions and cover stories. It invented a lone Romanian hacker named Guccifer 2.0 to take credit for the hacks; it also spread the rumors that a murdered DNC staffer named Seth Rich had leaked the emails from inside the organization—and it distributed many of the stolen documents through a fake whistle-blowing site called DCLeaks. Those deceptions became conspiracy theories, fanned by right-wing commentators and then-presidential candidate Donald Trump.

Read More

DEEP DIVE

The WIRED Guide to Cyberwar

ANDY GREENBERG

The deceptions generated a self-perpetuating ouroboros of mistrust: Skeptics dismissed even glaring clues of the Kremlin's guilt, like Russian-language formatting errors in the leaked documents, seeing those giveaways as planted evidence. Even a joint statement from US intelligence agencies four months later naming Russia as the perpetrator couldn't shake the conviction of disbelievers. They persist even today: In an *Economist*/YouGov poll earlier this year, only about half of Americans said they believed Russia interfered in the election.

With the malware that hit the Pyeongchang Olympics, the state of the art in digital deception took several evolutionary leaps forward. Investigators would find in its code not merely a single false flag but layers of false clues pointing at multiple potential culprits. And some of those clues were hidden deeper than any cybersecurity analyst had ever seen before.

From the start, the geopolitical motivations behind the Olympics sabotage were far from clear. The usual suspect for any cyberattack in South Korea is, of course, North Korea. The hermit kingdom has tormented its capitalist neighbors with military provocations and low-grade cyberwar for years. In the run-up to the Olympics, analysts at the cybersecurity firm McAfee had warned that Korean-speaking hackers had targeted the Pyeongchang Olympic organizers with phishing emails and what appeared to be espionage malware. At the time, McAfee analysts hinted in a phone call with me that North Korea was likely behind the spying scheme.

But there were contradictory signals on the public stage. As the Olympics began, the North seemed to be experimenting with a friendlier approach to geopolitics. The North Korean dictator, Kim Jong-un, had sent his sister as a diplomatic emissary to the games and had invited South Korea's president, Moon Jae-in, to visit the North Korean capital of Pyongyang. The two countries had even taken the surprising step of combining their Olympic women's hockey teams in a show of friendship. Why would North Korea launch a disruptive cyberattack in the midst of that charm offensive?

Then there was Russia. The Kremlin had its own motive for an attack on Pyeongchang. Investigations into doping by Russian athletes had led to a humiliating result in advance of the 2018 Olympics: Russia was banned. Its athletes would be allowed to compete but not to wear Russian flags or accept medals on behalf of their country. For years in the lead-up to that verdict, a state-sponsored Russian hacker team known as Fancy Bear had been retaliating, stealing and leaking data from Olympics-related targets. Russia's exile from the games was exactly the sort of slight that might inspire the Kremlin to unleash a piece of disruptive malware against the opening ceremony. If the Russian government couldn't enjoy the Olympics, then no one would.

If Russia had been trying to send a message with an attack on the Olympics' servers, however, it was hardly a direct one. Days before the opening ceremony, it had preemptively denied any Olympics-targeted hacking. "We know that Western media are planning pseudo-investigations on the theme of 'Russian fingerprints' in hacking attacks on information resources related to the hosting of the Winter Olympic Games in the Republic of Korea," Russia's Foreign Ministry had told Reuters. "Of course, no evidence will be presented to the world."

In fact, there would be plenty of evidence vaguely hinting at Russia's responsibility. The problem, it would soon become clear, was that there seemed to be just as much evidence pointing in a tangle of other directions too.

Three days after the opening ceremony, Cisco's Talos security division revealed that it had obtained a copy of Olympics-targeted malware and dissected it. Someone from the Olympics organizing committee or perhaps the Korean security firm AhnLab had uploaded the code to VirusTotal, a common database of malware samples used by cybersecurity analysts, where Cisco's reverse-engineers found it. The company published its findings in a [blog post](#) that would give that malware a name: Olympic Destroyer.

In broad outline, Cisco's description of Olympic Destroyer's anatomy called to mind two previous Russian cyberattacks, NotPetya and Bad Rabbit. As with those earlier attacks, Olympic Destroyer used a password-stealing tool, then combined those stolen passwords with remote access features in Windows that allowed it to spread among computers on a network. Finally, it used a data-destroying component to delete the boot configuration from infected machines before disabling all Windows services and shutting the computer down so that it couldn't be rebooted. Analysts at the security firm CrowdStrike would find other apparent Russian calling cards, elements that resembled a piece of Russian ransomware known as XData. Yet there seemed to be no clear code matches between Olympic Destroyer and the previous NotPetya or Bad Rabbit worms. Although it contained similar features, they had apparently been re-created from scratch or copied from elsewhere.

RELATED STORIES

After 6 Years in Exile, Edward Snowden Explains Himself

ANDY GREENBERG

BLACKOUT

New Clues Show Russia's Grid Hackers Aimed for Destruction

ANDY GREENBERG

HACKS

'Olympic Destroyer' Malware Hit Ahead of Opening Ceremony

ANDY GREENBERG

The deeper analysts dug, the stranger the clues became. The data-wiping portion of Olympic Destroyer shared characteristics with a sample of data-deleting code that had been used not by Russia but by the North Korean hacker group known as Lazarus. When Cisco researchers put the logical structures of the data-wiping components side by side, they seemed to roughly match. And both destroyed files with the same distinctive trick of deleting just their first 4,096 bytes. Was North Korea behind the attack after all?

There were still more signposts that led in completely different directions. The security firm Intezer noted that a chunk of the password-stealing code in Olympic Destroyer matched exactly with tools used by a hacker group known as APT3—a group that multiple cybersecurity firms have linked to the Chinese government. The company also traced a component that Olympic Destroyer used to generate encryption keys back to a third group, APT10, also reportedly linked to China. Intezer pointed out that the encryption component had never been used before by any other hacking teams, as far as the company's analysts could tell. Russia? North Korea? China? The more that forensic analysts reverse-engineered Olympic Destroyer's code, the further they seemed to get from arriving at a resolution.

In fact, all those contradictory clues seemed designed not to lead analysts toward any single false answer but to a collection of them, undermining any particular conclusion. The mystery became an epistemological crisis that left researchers doubting themselves. “It was psychological warfare on reverse-engineers,” says Silas Cutler, a security researcher who worked for CrowdStrike at the time. “It hooked into all those things you do as a backup check, that make you think ‘I know what this is.’ And it poisoned them.”

That self-doubt, just as much as the sabotage effects on the Olympics, seemed to have been the malware's true aim, says Craig Williams, a researcher at Cisco. “Even

as it accomplished its mission, it also sent a message to the security community,” Williams says. “*You can be misled.*”

The Olympics organizing committee, it turned out, wasn't Olympic Destroyer's only victim. According to the Russian security firm Kaspersky, the cyberattack also hit other targets with connections to the Olympics, including Atos, an IT services provider in France that had supported the event, and two ski resorts in Pyeongchang. One of those resorts had been infected seriously enough that its automated ski gates and ski lifts were temporarily paralyzed.

In the days after the opening ceremony attack, Kaspersky's Global Research and Analysis Team obtained a copy of the Olympic Destroyer malware from one of the ski resorts and began dusting it for fingerprints. But rather than focusing on the malware's code, as Cisco and Intezer had done, they looked at its “header,” a part of the file's metadata that includes clues about what sorts of programming tools were used to write it. Comparing that header with others in Kaspersky's vast database of malware samples, they found it perfectly matched the header of the North Korean Lazarus hackers' data-wiping malware—the same one Cisco had already pointed to as sharing traits with Olympic Destroyer. The North Korean theory seemed to be confirmed.

But one senior Kaspersky researcher named Igor Soumenkov decided to go a step further. Soumenkov, a hacker prodigy who'd been recruited to Kaspersky's research team as a teenager years earlier, had a uniquely deep knowledge of file headers, and he decided to double-check his colleagues' findings.

A tall, soft-spoken engineer, Soumenkov had a habit of arriving at work late in the morning and staying at Kaspersky's headquarters well after dark—a partially nocturnal schedule that he kept to avoid Moscow traffic.

One night, as his coworkers headed home, he pored over the code at a cubicle overlooking the city's jammed Leningradskoye Highway. By the end of that night, the traffic had thinned, he was virtually alone in the office, and he had determined that the header metadata didn't actually match other clues in the Olympic Destroyer

code itself; the malware hadn't been written with the programming tools that the header implied. The metadata had been forged.

This was something different from all the other signs of misdirection that researchers had fixated on. The other red herrings in Olympic Destroyer had been so vexing in part because there was no way to tell which clues were real and which were deceptions. But now, deep in the folds of false flags wrapped around the Olympic malware, Soumenkov had found one flag that was *provably* false. It was now clear that someone had tried to make the malware look North Korean and failed due to a slipup. It was only through Kaspersky's fastidious triple-checking that it came to light.

“It was psychological warfare on reverse-engineers.”

A few months later, I sat down with Soumenkov in a Kaspersky conference room in Moscow. Over an hour-long briefing, he explained in perfect English and with the clarity of a computer science professor how he'd defeated the attempted deception deep in Olympic Destroyer's metadata. I summarized what he seemed to have laid out for me: The Olympics attack clearly wasn't the work of North Korea. “It didn't look like them at all,” Soumenkov agreed.

And it certainly wasn't Chinese, I suggested, despite the more transparent false code hidden in Olympic Destroyer that fooled some researchers early on. “Chinese code is very recognizable, and this looks different,” Soumenkov agreed again.

Finally, I asked the glaring question: If not China, and not North Korea, then who? It seemed that the conclusion of that process of elimination was practically sitting there in the conference room with us and yet couldn't be spoken aloud.

Dig Deeper With Our Longreads Newsletter

Sign up to get our best longform features, investigations, and thought-provoking essays, in your inbox every Sunday.

Your email

Enter your email

SUBMIT

By signing up you agree to our [User Agreement](#) (including the [class action waiver and arbitration provisions](#)), our [Privacy Policy & Cookie Statement](#) and to receive marketing and account-related emails from WIRED. You can unsubscribe at any time.

“Ah, for that question, I brought a nice game,” Soumenkov said, affecting a kind of chipper tone. He pulled out a small black cloth bag and took out of it a set of dice. On each side of the small black cubes were written words like *Anonymous*, *Cybercriminals*, *Hacktivists*, *USA*, *China*, *Russia*, *Ukraine*, *Cyberterrorists*, *Iran*.

Kaspersky, like many other security firms, has a strict policy of only pinning attacks on hackers using the firm's own system of nicknames, never naming the country or government behind a hacking incident or hacker group—the safest way to avoid the murky and often political pitfalls of attribution. But the so-called attribution dice that Soumenkov held in his hand, which I'd seen before at hacker conferences, represented the most cynical exaggeration of the attribution problem: That no cyberattack can ever truly be traced to its source, and anyone who tries is simply guessing.

Soumenkov tossed the dice on the table. “Attribution is a tricky game,” he said. “Who is behind this? It's not our story, and it will never be.”

Michael Matonis was working from his home, a 400-square-foot basement apartment in the Washington, DC, neighborhood of Capitol Hill, when he first began to pull at the threads that would unravel Olympic Destroyer's mystery. The 28-year-old, a former anarchist punk turned security researcher with a controlled mass of curly black hair, had only recently moved to the city from upstate New York, and he still didn't have a desk at the Reston, Virginia, office of FireEye, the security and private intelligence firm that employed him. So on the day in February when he started to examine the malware that had struck Pyeongchang, Matonis was sitting at his makeshift workspace: a folding metal chair with his laptop propped up on a plastic table.

On a whim, Matonis decided to try a different approach from much of the rest of the perplexed security industry. He didn't search for clues in the malware's code.

Instead, in the days after the attack, Matonis looked at a far more mundane element of the operation: a fake, malware-laced Word document that had served as the first step in the nearly disastrous opening ceremony sabotage campaign.

The document, which appeared to contain a list of VIP delegates to the games, had likely been emailed to Olympics staff as an attachment. If anyone opened that attachment, it would run a malicious macro script that planted a backdoor on their PC, offering the Olympics hackers their first foothold on the target network. When Matonis pulled the infected document from VirusTotal, the malware repository where it had been uploaded by incident responders, he saw that the bait had likely been sent to Olympics staff in late November 2017, more than two months before the games began. The hackers had laid in wait for months before triggering their logic bomb.

Matonis began combing VirusTotal and FireEye's historical collection of malware, looking for matches to that code sample. On a first scan, he found none. But Matonis did notice that a few dozen malware-infected documents from the archives corresponded to his file's rough characteristics: They similarly carried embedded Word macros and, like the Olympics-targeted file, had been built to launch a certain common set of hacking tools called PowerShell Empire. The malicious Word macro traps, however, looked very different from one another, with their own unique layers of obfuscation.

Over the next two days, Matonis searched for patterns in that obfuscation that might serve as a clue. When he wasn't at his laptop, he'd turn the puzzle over in his mind, in the shower or lying on the floor of his apartment, staring up at the ceiling. Finally, he found a telling pattern in the malware specimens' encoding. Matonis declined to share with me the details of this discovery for fear of tipping off the hackers to their tell. But he could see that, like teenage punks who all pin just the right obscure band's buttons to their jackets and style their hair in the same shapes, the attempt to make the encoded files look unique had instead made one set of them a distinctly recognizable group. He soon deduced that the source of that signal in the noise was a common tool used to create each one of the booby-trapped documents. It was an open source program, easily found online, called Malicious Macro Generator.

SUBSCRIBE

Subscribe to WIRED and stay smart with more of your favorite writers.

Matonis speculated that the hackers had chosen the program in order to blend in with a crowd of other malware authors, but it had ultimately had the opposite effect, setting them apart as a distinct set. Beyond their shared tools, the malware group was also tied together by the author names Matonis pulled from the files' metadata: Almost all had been written by someone named either “AV,” “BD,” or “john.” When he looked at the command and control servers that the malware connected back to—the strings that would control the puppetry of any successful infections—all but a few of the IP addresses of those machines overlapped too. The fingerprints were hardly exact. But over the next days, he assembled a loose mesh of clues that added up to a solid net, tying the fake Word documents together.

Only after he had established those hidden connections did Matonis go back to the Word documents that had served as the vehicles for each malware sample and begin to Google-translate their contents, some written in Cyrillic. Among the files he'd tied to the Olympic Destroyer bait, Matonis found two other bait documents from the collection that dated back to 2017 and seemed to target Ukrainian LGBT activist groups, using infected files that pretended to be a gay rights organization's strategy document and a map of a Kiev Pride parade. Others targeted Ukrainian companies and government agencies with a tainted copy of draft legislation. This, for Matonis, was ominously familiar territory: For more than two years, he and the rest of the security industry had watched Russia launch a series of destructive

hacking operations against Ukraine, a relentless cyberwar that accompanied Russia's invasion of the country after its pro-Western 2014 revolution.

Even as that physical war had killed 13,000 people in Ukraine and displaced millions more, a Russian hacker group known as Sandworm had waged a full-blown cyberwar against Ukraine as well: It had barraged Ukrainian companies, government agencies, railways, and airports with wave after wave of data-destroying intrusions, including two unprecedented breaches of Ukrainian power utilities in 2015 and 2016 that had caused blackouts for hundreds of thousands of people. Those attacks culminated in NotPetya, a worm that had spread rapidly beyond Ukraine's borders and ultimately inflicted \$10 billion in damage on global networks, the most costly cyberattack in history.

In Matonis' mind, all other suspects for the Olympics attack fell away. Matonis couldn't yet connect the attack to any particular hacker group, but only one country would have been targeting Ukraine, nearly a year before the Pyeongchang attack, using the same infrastructure it would later use to hack the Olympics organizing committee—and it wasn't China or North Korea.

Strangely, other infected documents in the collection Matonis had unearthed seemed to target victims in the Russian business and real estate world. Had a team of Russian hackers been tasked with spying on some Russian oligarch on behalf of their intelligence taskmasters? Were they engaged in profit-focused cybercrime as a side gig?

Regardless, Matonis felt that he was on his way to finally, definitively cutting through the Olympics cyberattack's false flags to reveal its true origin: the Kremlin.

ILLUSTRATION: JOAN WONG

After Matonis had made those first, thrilling connections between Olympic Destroyer and a very familiar set of Russian hacking victims, he sensed he had explored beyond the part of Olympic Destroyer that its creators had intended for researchers to see—that he was now peering behind its curtain of false flags. He wanted to find out how much further he could go toward uncovering those hackers' full identities. So he told his boss that he wouldn't be coming into the FireEye office for the foreseeable future. For the next three weeks, he barely left his bunker apartment. He worked on his laptop from the same folding chair, with his back to the only window in his home that allowed in sunlight, poring over every data point that might reveal the next cluster of the hackers' targets.

A pre-internet-era detective might start a rudimentary search for a person by consulting phone books. Matonis started digging into the online equivalent, the directory of the web's global network known as the Domain Name System. DNS servers translate human-readable domains like facebook.com into the machine-readable IP addresses that describe the location of a networked computer that runs that site or service, like 69.63.176.13.

Matonis began painstakingly checking every IP address his hackers had used as a command and control server in their campaign of malicious Word document phishing; he wanted to see what domains those IP addresses had hosted. Since those domain names can move from machine to machine, he also used a reverse-lookup tool to flip the search—checking every name to see what other IP addresses had hosted it. He created a set of treelike maps connecting dozens of IP addresses and domain names linked to the Olympics attack. And far down the branch of one tree, a string of characters lit up like neon in Matonis' mind: account-loginserv.com.

A photographic memory can come in handy for an intelligence analyst. As soon as Matonis saw the account-loginserv.com domain, he instantly knew he had seen it nearly a year earlier in an FBI “flash”—a short alert sent out to US cybersecurity practitioners and potential victims. This one had offered a new detail about the hackers who, in 2016, had reportedly breached the Arizona and Illinois state boards of elections. These had been some of the most aggressive elements of Russia's meddling in US elections: Election officials had warned in 2016 that, beyond stealing and leaking emails from Democratic Party targets, Russian hackers had broken into the two states' voter rolls, accessing computers that held thousands of Americans' personal data with unknown intentions. According to the FBI flash alert Matonis had seen, the same intruders had also spoofed emails from a voting technology company, later reported to be the Tallahassee, Florida-based firm VR Systems, in an attempt to trick more election-related victims into giving up their passwords.

Matonis had found a fingerprint that linked the Olympics attackers back to a hacking operation that directly targeted the 2016 US election.

Matonis drew up a jumbled map of the connections on a piece of paper that he slapped onto his refrigerator with an Elvis magnet, and marveled at what he'd

found. Based on the FBI alert—and Matonis told me he confirmed the connection with another human source he declined to reveal—the fake VR Systems emails were part of a phishing campaign that seemed to have also used a spoofed login page at the account-loginserv.com domain he'd found in his Olympic Destroyer map. At the end of his long chain of internet-address connections, Matonis had found a fingerprint that linked the Olympics attackers back to a hacking operation that directly targeted the 2016 US election. Not only had he solved the whodunit of Olympic Destroyer's origin, he'd gone further, showing that the culprit had been implicated in the most notorious hacking campaign ever to hit the American political system.

Matonis had, since he was a teenager, been a motorcycle fan. When he was just barely old enough to ride one legally, he had scraped together enough money to buy a 1975 Honda CB750. Then one day a friend let him try riding his 2001 Harley-Davidson with an 1100 EVO engine. In three seconds, he was flying along a country road in upstate New York at 65 miles an hour, simultaneously fearing for his life and laughing uncontrollably.

When Matonis had finally outsmarted the most deceptive malware in history, he says he felt that same feeling, a rush that he could only compare to taking off on that Harley-Davidson in first gear. He sat alone in his DC apartment, staring at his screen and laughing.

By the time Matonis had drawn those connections, the US government had already drawn its own. The NSA and CIA, after all, have access to human spies and hacking abilities that no private-sector cybersecurity firm can rival. In late February, while Matonis was still holed up in his basement apartment, two unnamed intelligence officials told *The Washington Post* that the Olympics cyberattack had been carried out by Russia and that it had sought to frame North Korea. The anonymous officials went further, blaming the attack specifically on Russia's military intelligence agency, the GRU—the same agency that had masterminded the interference in the 2016 US election and the blackout attacks in Ukraine, and had unleashed NotPetya's devastation.

But as with most public pronouncements from inside the black box of the US intelligence apparatus, there was no way to check the government's work. Neither Matonis nor anyone else in media or cybersecurity research was privy to the trail the agencies had followed.

A set of US government findings that were far more useful and interesting to Matonis came months after his basement detective work. On July 13, 2018, special counsel Robert Mueller unsealed an indictment against 12 GRU hackers for engaging in election interference, laying out the evidence that they'd hacked the DNC and the Clinton campaign; the indictment even included details like the servers they'd used and the terms they'd typed into a search engine.

SIGN UP TODAY

Sign up for our Longreads newsletter for the best features and investigations on WIRED.

Deep in the 29-page indictment, Matonis read a description of the alleged activities of one GRU hacker named Anatoliy Sergeyevich Kovalev. Along with two other agents, Kovalev was named as a member of GRU Unit 74455, based in the northern Moscow suburb of Khimki in a 20-story building known as “the Tower.”

The indictment stated that Unit 74455 had provided backend servers for the GRU's intrusions into the DNC and the Clinton campaign. But more surprisingly, the indictment added that the group had “assisted in” the operation to leak the emails stolen in those operations. Unit 74455, the charges stated, had helped to set up DCLeaks.com and even Guccifer 2.0, the fake Romanian hacker persona that had

claimed credit for the intrusions and given the Democrats' stolen emails to WikiLeaks.

Kovalev, listed as 26 years old, was also accused of breaching one state's board of elections and stealing the personal information of some 500,000 voters. Later, he allegedly breached a voting systems company and then impersonated its emails in an attempt to hack voting officials in Florida with spoofed messages laced with malware. An FBI wanted poster for Kovalev showed a picture of a blue-eyed man with a slight smile and close-cropped, blond hair.

Though the indictment didn't say it explicitly, Kovalev's charges described exactly the activities outlined in the FBI flash alert that Matonis had linked to the Olympic Destroyer attack. Despite all of the malware's unprecedented deceptions and misdirections, Matonis could now tie Olympic Destroyer to a specific GRU unit, working at 22 Kirova Street in Khimki, Moscow, a tower of steel and mirrored glass on the western bank of the Moscow Canal.

A few months after Matonis shared those connections with me, in late November of 2018, I stood on a snow-covered path that wound along that frozen waterway on the outskirts of Moscow, staring up at the Tower.

I had, by then, been following the hackers known as Sandworm for two full years, and I was in the final stages of writing a book that investigated the remarkable arc of their attacks. I had traveled to Ukraine to interview the utility engineers who'd twice watched their power grids' circuit breakers be flipped open by unseen hands. I'd flown to Copenhagen to speak with sources at the shipping firm Maersk who whispered to me about the chaos that had unfolded when NotPetya paralyzed 17 of their terminals at ports around the globe, instantly shutting down the world's largest shipping conglomerate. And I'd sat with analysts from the Slovakian cybersecurity firm ESET in their office in Bratislava as they broke down their evidence that tied all of those attacks to a single group of hackers.

Beyond the connections in Matonis' branching chart and in the Mueller report that pinned the Olympics attack on the GRU, Matonis had shared with me other details

that loosely tied those hackers directly to Sandworm's earlier attacks. In some cases, they had placed command and control servers in data centers run by two of the same companies, Fortunix Networks and Global Layer, that had hosted servers used to trigger Ukraine's 2015 blackout and later the 2017 NotPetya worm. Matonis argued that those thin clues, on top of the vastly stronger case that all of those attacks were carried out by the GRU, suggested that Sandworm was, in fact, GRU Unit 74455. Which would put them in the building looming over me that snowy day in Moscow.

Read More

COVER STORY

The Untold Story of NotPetya, the Code that Crashed the World

ANDY GREENBERG AND EXCERPT

Standing there in the shadow of that opaque, reflective tower, I didn't know exactly what I hoped to accomplish. There was no guarantee that Sandworm's hackers were inside—they may have just as easily been split between that Khimki building and another GRU address named in the Mueller indictment, at 20 Komsomolskiy Prospekt, a building in central Moscow that I'd walked by that morning on my way to the train.

The Tower, of course, wasn't marked as a GRU facility. It was surrounded by an iron fence and surveillance cameras, with a sign at its gate that read GLAVNOYE UPRAVLENIYE OBUSTROYSTVA VOYSK—roughly, “General Directorate for the Arrangement of Troops.” I guessed that if I dared ask the guard at that gate if I could speak with someone from GRU Unit 74455, I was likely to end up detained in a room where I would be asked hard questions by Russian government officials, rather than the other way around.

This, I realized, might be the closest I had ever stood to Sandworm's hackers, and yet I could get no closer. A security guard appeared on the edge of the parking lot above me, looking out from within the Tower's fence—whether watching me or taking a smoke break, I couldn't tell. It was time for me to leave.

I walked north along the Moscow Canal, away from the Tower, and through the hush of the neighborhood's snow-padded parks and pathways to the nearby train station. On the train back to the city center, I glimpsed the glass building one last time, from the other side of the frozen water, before it was swallowed up in the Moscow skyline.

In early April of this year, I received an email via my Korean translator from Sang-jin Oh, the Korean official who led the response to Olympic Destroyer on the ground in Pyeongchang. He repeated what he'd said all along—that he would never discuss who might be responsible for the Olympics attack. He also noted that he and I wouldn't speak again: He'd moved on to a position in South Korea's Blue House, the office of the president, and wasn't authorized to take interviews. But in our final phone conversation months earlier, Oh's voice had still smoldered with anger when he recalled the opening ceremony and the 12 hours he'd spent desperately working to avert disaster.

“It still makes me furious that, without any clear purpose, someone hacked this event,” he'd said. “It would have been a huge black mark on these games of peace. I can only hope that the international community can figure out a way that this will never happen again.”

Even now, Russia's attack on the Olympics still haunts cyberwar wonks. (Russia's foreign ministry didn't respond to multiple requests for comment from WIRED.) Yes, the US government and the cybersecurity industry eventually solved the puzzle, after some initial false starts and confusion. But the attack set a new bar for deception, one that might still prove to have disastrous consequences when its tricks are repeated or evolve further, says Jason Healey, a cyberconflict-focused researcher at the Columbia School for International and Public Affairs

“Olympic Destroyer was the first time someone used false flags of that kind of sophistication in a significant, national-security-relevant attack,” Healey says. “It's a harbinger of what the conflicts of the future might look like.”

“If you can't imagine this with US and Russia, imagine it with India and Pakistan, or China and Taiwan, where a false flag provokes a much stronger response than intended.”

Healey, who worked in the George W. Bush White House as director for cyber infrastructure protection, says he has no doubt that US intelligence agencies can see through deceptive clues that muddy attribution. He's more worried about other countries where a misattributed cyberattack could have lasting consequences. “For the folks that can't afford CrowdStrike and FireEye, for the vast bulk of nations, attribution is still an issue,” Healey says. “If you can't imagine this with US and Russia, imagine it with India and Pakistan, or China and Taiwan, where a false flag provokes a much stronger response than even its authors intended, in a way that leaves the world looking very different afterwards.”

But false flags work here in the US, too, argues John Hultquist, the director of intelligence analysis at FireEye and Matonis' former boss before Matonis left the firm in July. Look no further, Hultquist says, than the half of Americans—or 73 percent of registered Republicans—who refuse to accept that Russia hacked the DNC or the Clinton campaign.

As the 2020 election approaches, Olympic Destroyer shows that Russia has only advanced its deception techniques—graduating from flimsy cover stories to the most sophisticated planted digital fingerprints ever seen. And if they can fool even a few researchers or reporters, they can sow even more of the public confusion that misled the American electorate in 2016. “The question is one of audience,” Hultquist says. “The problem is that the US government may never say a thing, and within 24 hours, the damage is done. The public was the audience in the first place.”

The GRU hackers known as Sandworm, meanwhile, are still out there. And Olympic Destroyer suggests they've been escalating not only their wanton acts of disruption but also their deception techniques. After years of crossing one red line after another, their next move is impossible to predict. But when those hackers do strike again, they may appear in a form we don't even recognize.

Source photos: Getty Images; Maxim Shemetov/Reuters (building)

From the book **SANDWORM**, by Andy Greenberg, to be published on November 5, 2019, by Doubleday, an imprint of the Knopf Doubleday Group, a division of Penguin Random House LLC. Copyright © 2019 by Andy Greenberg. Greenberg is a senior writer for WIRED.

This article appears in the November issue. [Subscribe now.](#)

Let us know what you think about this article. Submit a letter to the editor at mail@wired.com.

When you buy something using the retail links in our stories, we may earn a small affiliate commission. Read more about [how this works](#).

More Great WIRED Stories

- WIRED25: Stories of people [who are racing to save us](#)
- Massive, AI-powered robots [are 3D-printing entire rockets](#)
- *Ripper*—the inside story of the [egregiously bad videogame](#)
- USB-C has finally [come into its own](#)
- Planting tiny spy chips in hardware [can cost as little as \\$200](#)
- 👁 Prepare for the [deepfake era of video](#); plus, check out the [latest news on AI](#)
- 🏃 Want the best tools to get healthy? Check out our Gear team's picks for the [best fitness trackers](#), [running gear](#) (including [shoes](#) and [socks](#)), and [best headphones](#).



[Andy Greenberg](#) is a senior writer for WIRED, covering hacking, cybersecurity and surveillance. He's the author of the new book *[Tracers in the Dark: The Global Hunt for the Crime Lords of Cryptocurrency](#)*. His last book was *[Sandworm: A New Era of Cyberwar and the Hunt for the Kremlin's Most...](#)* [Read more](#)

SENIOR WRITER



TOPICS MAGAZINE-27.11 LONGREADS BOOK EXCERPT CYBERATTACKS OLYMPICS SOUTH KOREA RUSSIA

MORE FROM WIRED

Hackers Ran Amok Inside GoDaddy for Nearly 3 Years

Plus: The FBI got (at least a little bit) hacked, an election-disruption firm gets exposed, Russia mulls allowing “patriotic hacking,” and more.

ANDY GREENBERG

The Hunt for the Dark Web's Biggest Kingpin, Part 1: The Shadow

AlphaBay was the largest online drug bazaar in history, run by a technological mastermind who seemed untouchable—until his tech was turned against him.

ANDY GREENBERG

A New Kind of Bug Spells Trouble for iOS and macOS Security

Security researchers found a class of flaws that, if exploited, would allow an attacker to access people's messages, photos, and call history.

MATT BURGESS

The Push to Ban TikTok in the US Isn't About Privacy

Lawmakers are increasingly hellbent on punishing the popular social network while efforts to pass a broader privacy law have dwindled.

MATT LASLO

How to Unlock Your iPhone With a Security Key

Passcodes are out.

DAVID NIELD

How to Make Sure You're Not Accidentally Sharing Your Location

Keep your movements private.

DAVID NIELD

The TikTok Hearing Revealed That Congress Is the Problem

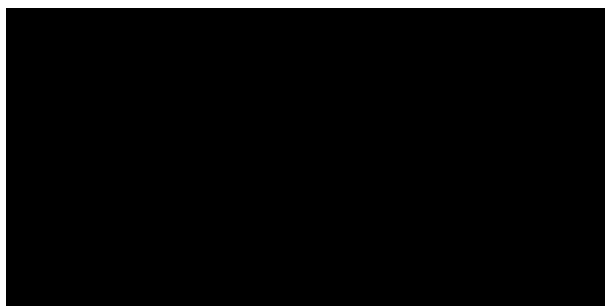
The interrogation of CEO Shou Zi Chew highlighted US lawmakers' own failure to pass privacy legislation.

DELL CAMERON

The Uniquely American Future of US Authoritarianism

The GOP-fueled far right differs from similar movements around the globe, thanks to the country's politics, electoral system, and changing demographics.

THOR BENSON



Internal Exhibit B

Vault 7: CIA Hacking Tools Revealed



Releases ▼ (index.html) **Documents ▼** (cms/index.html)

Contents

- Press Release
- Analysis
- Examples
- Frequently Asked Questions

Press Release

Today, Tuesday 7 March 2017, WikiLeaks begins its new series of leaks on the U.S. Central Intelligence Agency. Code-named "Vault 7" by WikiLeaks, it is the largest ever publication of confidential documents on the agency.

The first full part of the series, "Year Zero", comprises 8,761 documents and files from an isolated, high-security network situated inside the CIA's Center for Cyber Intelligence (files/org-chart.png) in Langley, Virginia. It follows an introductory disclosure last month of CIA targeting French political parties and candidates in the lead up to the 2012 presidential election (<https://wikileaks.org/cia-france-elections-2012>).

Recently, the CIA lost control of the majority of its hacking arsenal including malware, viruses, trojans, weaponized "zero day" exploits, malware remote control systems and associated documentation. This extraordinary collection, which amounts to more than several hundred million lines of code, gives its possessor the entire hacking capacity of the CIA. The archive appears to have been circulated among former U.S. government hackers and contractors in an unauthorized manner, one of whom has provided WikiLeaks with portions of the archive.

"Year Zero" introduces the scope and direction of the CIA's global covert hacking program, its malware arsenal and dozens of "zero day" weaponized exploits against a wide range of U.S. and European company products, include Apple's iPhone, Google's Android and Microsoft's Windows and even Samsung TVs, which are turned into covert microphones.

Since 2001 the CIA has gained political and budgetary preeminence over the U.S. National Security Agency (NSA). The CIA found itself building not just its now infamous drone fleet, but a very different type of covert, globe-spanning force — its own substantial fleet of hackers. The agency's hacking division freed it from having to disclose its often controversial operations to the NSA (its primary bureaucratic rival) in order to draw on the NSA's hacking capacities.

By the end of 2016, the CIA's hacking division, which formally falls under the agency's Center for Cyber Intelligence (files/org-chart.png) (CCI), had over 5000 registered users and had produced more than a thousand hacking systems, trojans, viruses, and other "weaponized" malware. Such is the scale of the CIA's undertaking that by 2016, its hackers had utilized more code than that used to run Facebook. The CIA had created, in effect, its "own NSA" with even less accountability and without

publicly answering the question as to whether such a massive budgetary spend on duplicating the capacities of a rival agency could be justified.

In a statement to WikiLeaks the source details policy questions that they say urgently need to be debated in public, including whether the CIA's hacking capabilities exceed its mandated powers and the problem of public oversight of the agency. The source wishes to initiate a public debate about the security, creation, use, proliferation and democratic control of cyberweapons.

Once a single cyber 'weapon' is 'loose' it can spread around the world in seconds, to be used by rival states, cyber mafia and teenage hackers alike.

Julian Assange, WikiLeaks editor stated that "There is an extreme proliferation risk in the development of cyber 'weapons'.

Comparisons can be drawn between the uncontrolled proliferation of such 'weapons', which results from the inability to contain them combined with their high market value, and the global arms trade. But the significance of "Year Zero" goes well beyond the choice between cyberwar and cyberpeace. The disclosure is also exceptional from a political, legal and forensic perspective."

Wikileaks has carefully reviewed the "Year Zero" disclosure and published substantive CIA documentation while avoiding the distribution of 'armed' cyberweapons until a consensus emerges on the technical and political nature of the CIA's program and how such 'weapons' should analyzed, disarmed and published.

Wikileaks has also decided to redact and anonymise some identifying information in "Year Zero" for in depth analysis. These redactions include ten of thousands of CIA targets and attack machines throughout Latin America, Europe and the United

States. While we are aware of the imperfect results of any approach chosen, we remain committed to our publishing model and note that the quantity of published pages in "Vault 7" part one ("Year Zero") already eclipses the total number of pages published over the first three years of the Edward Snowden NSA leaks.

Analysis

CIA malware targets iPhone, Android, smart TVs

CIA malware and hacking tools are built by EDG (Engineering Development Group), a software development group within CCI (Center for Cyber Intelligence), a department belonging to the CIA's DDI (Directorate for Digital Innovation). The DDI is one of the five major directorates of the CIA (see this organizational chart (files/org-chart.png) of the CIA for more details).

The EDG is responsible for the development, testing and operational support of all backdoors, exploits, malicious payloads, trojans, viruses and any other kind of malware used by the CIA in its covert operations world-wide.

The increasing sophistication of surveillance techniques has drawn comparisons with George Orwell's 1984, but "Weeping Angel", developed by the CIA's Embedded Devices Branch (EDB) (cms/space_753667.html), which infests smart TVs, transforming them into covert microphones, is surely its most emblematic realization.

The attack against Samsung smart TVs (cms/page_12353643.html) was developed in cooperation with the United Kingdom's MI5/BTSS. After infestation, Weeping Angel places the target TV in a 'Fake-Off' mode, so that the owner

falsely believes the TV is off when it is on. In 'Fake-Off' mode the TV operates as a bug, recording conversations in the room and sending them over the Internet to a covert CIA server.

As of October 2014 the CIA was also looking at infecting the vehicle control systems used by modern cars and trucks (cms/page_13763790.html). The purpose of such control is not specified, but it would permit the CIA to engage in nearly undetectable assassinations.

The CIA's Mobile Devices Branch (MDB) developed numerous attacks to remotely hack and control popular smart phones (cms/space_3276804.html). Infected phones can be instructed to send the CIA the user's geolocation, audio and text communications as well as covertly activate the phone's camera and microphone.

Despite iPhone's minority share (14.5%) of the global smart phone market in 2016, a specialized unit in the CIA's Mobile Development Branch produces malware to infest, control and exfiltrate data from iPhones and other Apple products running iOS, such as iPads (cms/space_2359301.html). CIA's arsenal includes numerous local and remote "zero days" (cms/page_13205587.html) developed by CIA or obtained from GCHQ, NSA, FBI or purchased from cyber arms contractors such as Baitshop. The disproportionate focus on iOS may be explained by the popularity of the iPhone among social, political, diplomatic and business elites.

A similar unit targets Google's Android which is used to run the majority of the world's smart phones (~85%) including Samsung, HTC and Sony (cms/space_11763721.html). 1.15 billion Android powered phones were sold last year. "Year Zero" shows that as of

2016 the CIA had 24 "weaponized" Android "zero days" (cms/page_11629096.html) which it has developed itself and obtained from GCHQ, NSA and cyber arms contractors.

These techniques permit the CIA to bypass the encryption of WhatsApp, Signal, Telegram, Wiebo, Confide and Cloackman by hacking the "smart" phones that they run on and collecting audio and message traffic before encryption is applied.

CIA malware targets Windows, OSx, Linux, routers

The CIA also runs a very substantial effort to infect and control Microsoft Windows users (cms/page_11628612.html) with its malware. This includes multiple local and remote weaponized "zero days", air gap jumping viruses such as "Hammer Drill" (cms/page_17072172.html) which infects software distributed on CD/DVDs, infectors for removable media such as USBs (cms/page_13762636.html), systems to hide data in images (cms/page_13763247.html) or in covert disk areas ("Brutal Kangaroo" (cms/page_13763236.html)) and to keep its malware infestations going (cms/page_13763650.html).

Many of these infection efforts are pulled together by the CIA's Automated Implant Branch (AIB) (cms/space_3276805.html), which has developed several attack systems for automated infestation and control of CIA malware, such as "Assassin" and "Medusa".

Attacks against Internet infrastructure and web servers are developed by the CIA's Network Devices Branch (NDB) (cms/space_15204355.html).

The CIA has developed automated multi-platform malware attack and control systems covering Windows, Mac OS X, Solaris, Linux and more, such as EDB's "HIVE" and the related "Cutthroat" and "Swindle" tools, which are described in the examples section below.

CIA 'hoarded' vulnerabilities ("zero days")

In the wake of Edward Snowden's leaks about the NSA, the U.S. technology industry secured a commitment from the Obama administration that the executive would disclose on an ongoing basis — rather than hoard — serious vulnerabilities, exploits, bugs or "zero days" to Apple, Google, Microsoft, and other US-based manufacturers.

Serious vulnerabilities not disclosed to the manufacturers places huge swathes of the population and critical infrastructure at risk to foreign intelligence or cyber criminals who independently discover or hear rumors of the vulnerability. If the CIA can discover such vulnerabilities so can others.

The U.S. government's commitment to the Vulnerabilities Equities Process (<https://is.gd/vepvpep>) came after significant lobbying by US technology companies, who risk losing their share of the global market over real and perceived hidden vulnerabilities. The government stated that it would disclose all pervasive vulnerabilities discovered after 2010 on an ongoing basis.

"Year Zero" documents show that the CIA breached the Obama administration's commitments. Many of the vulnerabilities used in the CIA's cyber arsenal are pervasive and some may already have been found by rival intelligence agencies or cyber criminals.

As an example, specific CIA malware revealed in "Year Zero" is able to penetrate, infest and control both the Android phone and iPhone software that runs or has run presidential Twitter accounts. The CIA attacks this software by using undisclosed security vulnerabilities ("zero days") possessed by the CIA but if the CIA can hack these phones then so can everyone else who has obtained or discovered the vulnerability. As long as the CIA keeps these vulnerabilities concealed from Apple and Google (who make the phones) they will not be fixed, and the phones will remain hackable.

The same vulnerabilities exist for the population at large, including the U.S. Cabinet, Congress, top CEOs, system administrators, security officers and engineers. By hiding these security flaws from manufacturers like Apple and Google the CIA ensures that it can hack everyone &mdsh; at the expense of leaving everyone hackable.

'Cyberwar' programs are a serious proliferation risk

Cyber 'weapons' are not possible to keep under effective control.

While nuclear proliferation has been restrained by the enormous costs and visible infrastructure involved in assembling enough fissile material to produce a critical nuclear mass, cyber 'weapons', once developed, are very hard to retain.

Cyber 'weapons' are in fact just computer programs which can be pirated like any other. Since they are entirely comprised of information they can be copied quickly with no marginal cost.

Securing such 'weapons' is particularly difficult since the same people who develop and use them have the skills to exfiltrate copies without leaving traces — sometimes by using the very same 'weapons' against the organizations that contain them. There are substantial price incentives for government hackers and consultants to obtain copies since there is a global "vulnerability market" that will pay hundreds of thousands to millions of dollars for copies of such 'weapons'. Similarly, contractors and companies who obtain such 'weapons' sometimes use them for their own purposes, obtaining advantage over their competitors in selling 'hacking' services.

Over the last three years the United States intelligence sector, which consists of government agencies such as the CIA and NSA and their contractors, such as Booz Allan Hamilton, has been subject to unprecedented series of data exfiltrations by its own workers.

A number of intelligence community members not yet publicly named have been arrested or subject to federal criminal investigations in separate incidents.

Most visibly, on February 8, 2017 a U.S. federal grand jury indicted Harold T. Martin III with 20 counts of mishandling classified information. The Department of Justice alleged that it seized some 50,000 gigabytes of information from Harold T. Martin III that he had obtained from classified programs at NSA and CIA, including the source code for numerous hacking tools.

Once a single cyber 'weapon' is 'loose' it can spread around the world in seconds, to be used by peer states, cyber mafia and teenage hackers alike.

U.S. Consulate in Frankfurt is a covert CIA hacker base

In addition to its operations in Langley, Virginia the CIA also uses the U.S. consulate in Frankfurt as a covert base for its hackers covering Europe, the Middle East and Africa.

CIA hackers operating out of the Frankfurt consulate ("Center for Cyber Intelligence Europe" (cms/page_20251151.html) or CCIE) are given diplomatic ("black") passports and State Department cover. The instructions for incoming CIA hackers (cms/page_26607630.html) make Germany's counter-intelligence efforts appear inconsequential: "Breeze through German Customs because you have your cover-for-action story down pat, and all they did was stamp your passport"

Your Cover Story (for this trip)

Q: Why are you here?

A: Supporting technical consultations at the Consulate.

Two earlier WikiLeaks publications give further detail on CIA approaches to customs (/cia-travel/) and secondary screening procedures (/cia-travel/).

Once in Frankfurt CIA hackers can travel without further border checks to the 25 European countries that are part of the Shengen open border area — including France, Italy and Switzerland.

A number of the CIA's electronic attack methods are designed for physical proximity. These attack methods are able to penetrate high security networks that are disconnected from the internet, such as police record database. In these cases, a CIA officer, agent or allied intelligence officer acting under instructions, physically infiltrates the targeted workplace. The attacker is provided with a USB containing malware developed for the CIA for this purpose, which is inserted into the targeted computer. The

attacker then infects and exfiltrates data to removable media. For example, the CIA attack system Fine Dining (cms/page_20251107.html), provides 24 decoy applications for CIA spies to use. To witnesses, the spy appears to be running a program showing videos (e.g VLC), presenting slides (Prezi), playing a computer game (Breakout2, 2048) or even running a fake virus scanner (Kaspersky, McAfee, Sophos). But while the decoy application is on the screen, the underlaying system is automatically infected and ransacked.

How the CIA dramatically increased proliferation risks

In what is surely one of the most astounding intelligence own goals in living memory, the CIA structured its classification regime such that for the most market valuable part of "Vault 7" — the CIA's weaponized malware (implants + zero days), Listening Posts (LP), and Command and Control (C2) systems — the agency has little legal recourse.

The CIA made these systems unclassified.

Why the CIA chose to make its cyberarsenal unclassified reveals how concepts developed for military use do not easily crossover to the 'battlefield' of cyber 'war'.

To attack its targets, the CIA usually requires that its implants communicate with their control programs over the internet. If CIA implants, Command & Control and Listening Post software were classified, then CIA officers could be prosecuted or dismissed for violating rules that prohibit placing classified information onto the Internet. Consequently the CIA has secretly made most of its cyber spying/war code unclassified. The U.S. government is not able to assert copyright either, due to restrictions in the U.S.

Constitution. This means that cyber 'arms' manufactures and computer hackers can freely "pirate" these 'weapons' if they are obtained. The CIA has primarily had to rely on obfuscation to protect its malware secrets.

Conventional weapons such as missiles may be fired at the enemy (i.e into an unsecured area). Proximity to or impact with the target detonates the ordnance including its classified parts. Hence military personnel do not violate classification rules by firing ordnance with classified parts. Ordnance will likely explode. If it does not, that is not the operator's intent.

Over the last decade U.S. hacking operations have been increasingly dressed up in military jargon to tap into Department of Defense funding streams. For instance, attempted "malware injections" (commercial jargon) or "implant drops" (NSA jargon) are being called "fires" as if a weapon was being fired. However the analogy is questionable.

Unlike bullets, bombs or missiles, most CIA malware is designed to live for days or even years after it has reached its 'target'. CIA malware does not "explode on impact" but rather permanently infests its target. In order to infect target's device, copies of the malware must be placed on the target's devices, giving physical possession of the malware to the target. To exfiltrate data back to the CIA or to await further instructions the malware must communicate with CIA Command & Control (C2) systems placed on internet connected servers. But such servers are typically not approved to hold classified information, so CIA command and control systems are also made unclassified.

A successful 'attack' on a target's computer system is more like a series of complex stock maneuvers in a hostile take-over bid or the careful planting of rumors in order to gain control over an

organization's leadership rather than the firing of a weapons system. If there is a military analogy to be made, the infestation of a target is perhaps akin to the execution of a whole series of military maneuvers against the target's territory including observation, infiltration, occupation and exploitation.

Evading forensics and anti-virus

A series of standards lay out CIA malware infestation patterns which are likely to assist forensic crime scene investigators as well as Apple, Microsoft, Google, Samsung, Nokia, Blackberry, Siemens and anti-virus companies attribute and defend against attacks.

"Tradecraft DO's and DON'Ts" ([cms/page_14587109.html](https://wikileaks.org/ciav7p1/cms/page_14587109.html)) contains CIA rules on how its malware should be written to avoid fingerprints implicating the "CIA, US government, or its witting partner companies" in "forensic review". Similar secret standards cover the use of encryption to hide CIA hacker and malware communication

([cms/files/NOD%20Cryptographic%20Requirements%20v1.1%20TOP%20SECRET.pdf](https://wikileaks.org/ciav7p1/cms/files/NOD%20Cryptographic%20Requirements%20v1.1%20TOP%20SECRET.pdf)) (pdf), describing targets & exfiltrated data ([cms/files/Codex-Spec-v1-SECRET.pdf](https://wikileaks.org/ciav7p1/cms/files/Codex-Spec-v1-SECRET.pdf)) (pdf) as well as executing payloads ([cms/files/ICE-Spec-v3-final-SECRET.pdf](https://wikileaks.org/ciav7p1/cms/files/ICE-Spec-v3-final-SECRET.pdf)) (pdf) and persisting ([cms/files/Persisted-DLL-Spec-v2-SECRET.pdf](https://wikileaks.org/ciav7p1/cms/files/Persisted-DLL-Spec-v2-SECRET.pdf)) (pdf) in the target's machines over time.

CIA hackers developed successful attacks against most well known anti-virus programs. These are documented in AV defeats ([cms/page_2064514.html](https://wikileaks.org/ciav7p1/cms/page_2064514.html)), Personal Security Products ([cms/page_13762910.html](https://wikileaks.org/ciav7p1/cms/page_13762910.html)), Detecting and defeating PSPs ([cms/page_7995642.html](https://wikileaks.org/ciav7p1/cms/page_7995642.html)) and PSP/Debugger/RE Avoidance ([cms/page_2621845.html](https://wikileaks.org/ciav7p1/cms/page_2621845.html)). For example, Comodo was defeated

by CIA malware placing itself in the Window's "Recycle Bin" (cms/page_5341269.html). While Comodo 6.x has a "Gaping Hole of DOOM" (cms/page_5341272.html).

CIA hackers discussed what the NSA's "Equation Group" hackers did wrong and how the CIA's malware makers could avoid similar exposure (cms/page_14588809.html).

Examples

The CIA's Engineering Development Group (EDG) management system contains around 500 different projects (only some of which are documented by "Year Zero") each with their own sub-projects, malware and hacker tools.

The majority of these projects relate to tools that are used for penetration, infestation ("implanting"), control, and exfiltration.

Another branch of development focuses on the development and operation of Listening Posts (LP) and Command and Control (C2) systems used to communicate with and control CIA implants; special projects are used to target specific hardware from routers to smart TVs.

Some example projects are described below, but see the table of contents (cms/index.html) for the full list of projects described by WikiLeaks' "Year Zero".

UMBAGE

The CIA's hand crafted hacking techniques pose a problem for the agency. Each technique it has created forms a "fingerprint" that can be used by forensic investigators to attribute multiple different attacks to the same entity.

This is analogous to finding the same distinctive knife wound on multiple separate murder victims. The unique wounding style creates suspicion that a single murderer is responsible. As soon one murder in the set is solved then the other murders also find likely attribution.

The CIA's Remote Devices Branch (cms/space_753668.html)'s UMBAGE group (cms/page_2621751.html) collects and maintains a substantial library (cms/page_2621753.html) of attack techniques 'stolen' from malware produced in other states including the Russian Federation.

With UMBAGE and related projects the CIA cannot only increase its total number of attack types but also misdirect attribution by leaving behind the "fingerprints" of the groups that the attack techniques were stolen from.

UMBAGE components cover keyloggers, password collection, webcam capture, data destruction, persistence, privilege escalation, stealth, anti-virus (PSP) avoidance and survey techniques.

Fine Dining

Fine Dining comes with a standardized questionnaire i.e menu that CIA case officers fill out. The questionnaire is used by the agency's OSB (Operational Support Branch (cms/space_1736706.html)) to transform the requests of case

officers into technical requirements for hacking attacks (typically "exfiltrating" information from computer systems) for specific operations. The questionnaire allows the OSB to identify how to adapt existing tools for the operation, and communicate this to CIA malware configuration staff. The OSB functions as the interface between CIA operational staff and the relevant technical support staff.

Among the list of possible targets of the collection are 'Asset', 'Liason Asset', 'System Administrator', 'Foreign Information Operations', 'Foreign Intelligence Agencies' and 'Foreign Government Entities'. Notably absent is any reference to extremists or transnational criminals. The 'Case Officer' is also asked to specify the environment of the target like the type of computer, operating system used, Internet connectivity and installed anti-virus utilities (PSPs) as well as a list of file types to be exfiltrated like Office documents, audio, video, images or custom file types. The 'menu' also asks for information if recurring access to the target is possible and how long unobserved access to the computer can be maintained. This information is used by the CIA's 'JQJIMPROVISE' software (see below) to configure a set of CIA malware suited to the specific needs of an operation.

Improvise (JQJIMPROVISE)

'Improvise' is a toolset for configuration, post-processing, payload setup and execution vector selection for survey/exfiltration tools supporting all major operating systems like Windows (Bartender), MacOS (JukeBox) and Linux (DanceFloor). Its configuration utilities like Margarita allows the NOC (Network Operation Center) to customize tools based on requirements from 'Fine Dining' questionnaires.

HIVE

HIVE is a multi-platform CIA malware suite and its associated control software. The project provides customizable implants for Windows, Solaris, MikroTik (used in internet routers) and Linux platforms and a Listening Post (LP)/Command and Control (C2) infrastructure to communicate with these implants.

The implants are configured to communicate via HTTPS with the webserver of a cover domain; each operation utilizing these implants has a separate cover domain and the infrastructure can handle any number of cover domains.

Each cover domain resolves to an IP address that is located at a commercial VPS (Virtual Private Server) provider. The public-facing server forwards all incoming traffic via a VPN to a 'Blot' server that handles actual connection requests from clients. It is setup for optional SSL client authentication: if a client sends a valid client certificate (only implants can do that), the connection is forwarded to the 'Honeycomb' toolserver that communicates with the implant; if a valid certificate is missing (which is the case if someone tries to open the cover domain website by accident), the traffic is forwarded to a cover server that delivers an unsuspecting looking website.

The Honeycomb toolserver receives exfiltrated information from the implant; an operator can also task the implant to execute jobs on the target computer, so the toolserver acts as a C2 (command and control) server for the implant.

Similar functionality (though limited to Windows) is provided by the RickBobby project.

See the classified user (cms/files/UsersGuide.pdf) and developer (cms/files/DevelopersGuide.pdf) guides for HIVE.

Frequently Asked Questions

Why now?

WikiLeaks published as soon as its verification and analysis were ready.

In February the Trump administration has issued an Executive Order calling for a "Cyberwar" review to be prepared within 30 days.

While the review increases the timeliness and relevance of the publication it did not play a role in setting the publication date.

Redactions

Names, email addresses and external IP addresses have been redacted in the released pages (70,875 redactions in total) until further analysis is complete.

1. **Over-redaction:** Some items may have been redacted that are not employees, contractors, targets or otherwise related to the agency, but are, for example, authors of documentation for otherwise public projects that are used by the agency.
2. **Identity vs. person:** the redacted names are replaced by user IDs (numbers) to allow readers to assign multiple pages to a single author. Given the redaction process used

a single person may be represented by more than one assigned identifier but no identifier refers to more than one real person.

3. **Archive attachments (zip, tar.gz, ...)** are replaced with a PDF listing all the file names in the archive. As the archive content is assessed it may be made available; until then the archive is redacted.
4. **Attachments with other binary content** are replaced by a hex dump of the content to prevent accidental invocation of binaries that may have been infected with weaponized CIA malware. As the content is assessed it may be made available; until then the content is redacted.
5. The **tens of thousands of routable IP addresses references** (including more than 22 thousand within the United States) that correspond to possible targets, CIA covert listening post servers, intermediary and test systems, are redacted for further exclusive investigation.
6. **Binary files of non-public origin** are only available as dumps to prevent accidental invocation of CIA malware infected binaries.

Organizational Chart

The organizational chart (files/org-chart.png) corresponds to the material published by WikiLeaks so far.

Since the organizational structure of the CIA below the level of Directorates is not public, the placement of the EDG and its branches within the org chart of the agency is reconstructed from information contained in the documents released so far. It is

intended to be used as a rough outline of the internal organization; please be aware that the reconstructed org chart is incomplete and that internal reorganizations occur frequently.

Wiki pages

"Year Zero" contains 7818 web pages with 943 attachments from the internal development groupware. The software used for this purpose is called Confluence, a proprietary software from Atlassian. Webpages in this system (like in Wikipedia) have a version history that can provide interesting insights on how a document evolved over time; the 7818 documents include these page histories for 1136 latest versions.

The order of named pages within each level is determined by date (oldest first). Page content is not present if it was originally dynamically created by the Confluence software (as indicated on the re-constructed page).

What time period is covered?

The years 2013 to 2016. The sort order of the pages within each level is determined by date (oldest first).

WikiLeaks has obtained the CIA's creation/last modification date for each page but these do not yet appear for technical reasons. Usually the date can be discerned or approximated from the content and the page order. If it is critical to know the exact time/date contact WikiLeaks.

What is "Vault 7"

"Vault 7" is a substantial collection of material about CIA activities obtained by WikiLeaks.

When was each part of "Vault 7" obtained?

Part one was obtained recently and covers through 2016. Details on the other parts will be available at the time of publication.

Is each part of "Vault 7" from a different source?

Details on the other parts will be available at the time of publication.

What is the total size of "Vault 7"?

The series is the largest intelligence publication in history.

How did WikiLeaks obtain each part of "Vault 7"?

Sources trust WikiLeaks to not reveal information that might help identify them.

Isn't WikiLeaks worried that the CIA will act against its staff to stop the series?

No. That would be certainly counter-productive.

Has WikiLeaks already 'mined' all the best stories?

No. WikiLeaks has intentionally not written up hundreds of impactful stories to encourage others to find them and so create expertise in the area for subsequent parts in the series. They're there. Look. Those who demonstrate journalistic excellence may be considered for early access to future parts.

Won't other journalists find all the best stories before me?

Unlikely. There are very considerably more stories than there are journalists or academics who are in a position to write them.

Top



WL Research Community - user contributed research based on documents published by WikiLeaks.

(<https://our.wikileaks.org>)

Tor is an encrypted anonymising network that makes it harder to intercept internet communications, or see where communications are coming from or going to.

(<https://www.torproject.org>)

Tails is a live operating system, that you can start on almost any computer from a DVD, USB stick, or SD card. It aims at preserving your privacy and anonymity.

(<https://tails.boum.org/>)

The Courage Foundation is an international organisation that supports those who risk life or liberty to make significant contributions to the historical record.

(<https://www.couragefoundation.org/>)

Bitcoin uses peer-to-peer technology to operate with no central authority or banks; managing transactions and the issuing of bitcoins is carried out collectively by the network.

(<https://www.bitcoin.org/>)



(<https://www.facebook.com/wikileaks>)



(<https://twitter.com/wikileaks>)

Internal Exhibit C



Sign in



Search the web



My Feed

News



Personalize



AdChoices



Washington Examiner

+ Follow

View Profile

Twitter and Meta take down pro-U.S. propaganda campaign targeting Middle East

Story by Brady Knox • Aug 26, 2022



Twitter and Meta take down pro-U.S. propaganda campaign targeting Middle East
© Provided by Washington Examiner

Twitter and Meta took down a sprawling network of accounts involved in a covert pro-United States propaganda campaign targeting the Middle East, Iran, Central Asia, and Afghanistan.

A research paper written by the intelligence company Graphika and Stanford Internet Observatory documented a network of hundreds of accounts across several different social media networks, including Twitter, Instagram, Facebook, Telegram, YouTube, and more. These accounts targeted U.S. adversaries, mainly Russia, China, and Iran, creating fake personas and organizations to spread narratives against them in contested areas such as Central Asia and the Middle East.



Explore The Latest Trends -
Shop Macy's VIP Sale Now

Twitter and Meta didn't speculate as to who or what was behind the network, only saying that it likely originated in the U.S. or United Kingdom.

TIKTOK OWNER BYTEDANCE PROMOTED PRO-CHINA CONTENT ON NEWS AGGREGATOR APP

The campaign, waged mostly after 2017 up until its termination in August 2022, was found to be mostly ineffective, with the majority of the posts only generating limited interaction. However, a few posts gained significant traction. A video produced and posted by a sham news account from the

Continue reading

SPONSORED CONTENT



Monthly Bookkeeping
\$95/Month - QB Pro
Certified Bookkeepers

Ad www.remotebooksonline.com...



Hands Free Sneakers,
Adjustable Arch Support,
Easy On/Off, Wide Toe-Box,...

Ad Orthofeet

More for You



1 Comfortable Pronation
Sneakers, Premium Arch
Support, Tieless Shoelaces,...

Ad Orthofeet



Slip On Tennis Shoes,
Customized Arch Support,
Pain Relief Technology,...

Ad Orthofeet

Find the Best Real Estate Now - Find the Right Home for You

Ad homes.mitula.com/Search/Top-10



2Paragraphs

Tim Tebow's Wife Flaunts
Legs With Jessie James
Decker 'What a Squad'

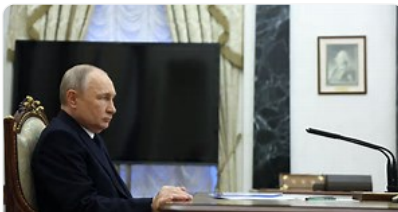
218 409 23



Newsweek

Bryan Kohberger's Drastic
Change Behind Bars—
Reports

233 1k 288



Newsweek

China Responds to Putin's
Threat to Break Nuclear
Weapons Pledge

507 332 164



Daily Mail

Female school shooter
Nashville is just the
history

103 805 645



USA TODAY

Flights grounded, labor
union strike: Netanyahu
pauses judicial reform amid...

985 299 247



USA TODAY

A Florida plastic surgeon
sued his former employer.
Now he's accused of...

4 13



Wholesale Green Coffee
Beans - FREE
Shipping|Wholesale Prices

Ad www.genuineorigin.com/gree...



Why Their Marriage
Lasted Centuries

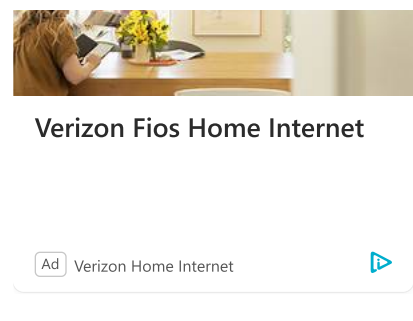
Ad Definition.org



© 2023 Microsoft

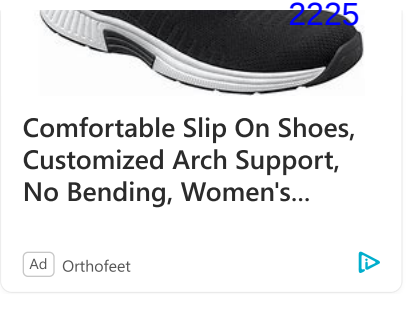
Privacy & Cookies Terms of use Advertise

Feedback



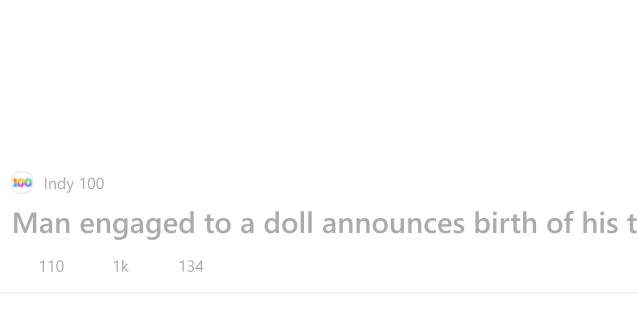
Verizon Fios Home Internet

Ad Verizon Home Internet




Comfortable Slip On Shoes, Customized Arch Support, No Bending, Women's...

Ad Orthofeet



Man engaged to a doll announces birth of his t

110 1k 134



The Daily Digest [+ Follow](#) [View Profile](#)


Which Democrat could run instead of Joe Biden in 2024?

Story by Zeleb.es • 1h ago

57

21

71



Auto Rotation Off ☐

1 of 21 Photos in Gallery

No more Uncle Joe?

Everything seems to be in place for Joe Biden to run in the 2024 Presidential Election except for one thing: the people. An Associated Poll released on February 2023 reveals that only 37% of voters identified as Democrats want four more years of Uncle Joe.

SPONSORED CONTENT

More for You

Internal Exhibit D



FAITH NEWS

Hackers planted false files implicating Indian Jesuit Father Swamy who died in prison

Catholic News Service
December 15, 2022

NEW DELHI (CNS)—Catholic activists and priests want the Indian government to “take full responsibility” for the custodial [death of Jesuit Father Stan Swamy](#) after findings by U.S. -based digital forensic experts that false evidence was planted on the priest’s computer.

In a recent report, Arsenal Consulting, a Massachusetts-based digital forensics firm, said the “digital evidence used to arrest senior human rights defender Father Swamy in the Bhima-Koregaon case was planted on his computer’s hard drive.”

ADVERTISEMENT

The 84-year-old Jesuit, a rights activist based in eastern Jharkhand state, died in a hospital while imprisoned in Mumbai in July 2021 after being denied bail on medical grounds, despite suffering from multiple age-related ailments.

He was arrested Oct. 8, 2020, by India’s anti-terror National Investigation Agency and accused of being party to a conspiracy allegedly hatched by outlawed Maoist rebels to unleash mob violence at Bhima-Koregaon, in the western state of Maharashtra, Jan. 1, 2018.

Ucanews.com reported Arsenal said “the attacker responsible for compromising Father Swamy’s computer had extensive resources (including time), and it is obvious that the primary goals were surveillance and incriminating document delivery.”

ADVERTISEMENT

Read more from America



Cardinal Gregory:
Pope Francis
makes Americans...
Kate Scanlon - OSV
News

Why an 84-year-old Indian Jesuit—Fr. Stan Swamy—is in prison



Disclosing details of the findings, Jesuit Father Joseph Xavier said in a statement that the hackers “first attacked Father Swamy’s computer on Oct. 19, 2014, using a Remote Access Trojan (RAT) called Netwire.”

“The report (by Arsenal) shows examples of the hackers being able to read his passwords as he was typing them, as well as other documents and emails,” said Father Xavier, who is also a convener of the Father Stan Swamy Legacy Committee of the Jesuits.

ADVERTISEMENT

The hacker also read as many as 24,000 files on Father Stan’s device and planted files between July 2017 and June 2019, Father Xavier said, quoting from the report.

“Over 50 files were created on Father Swamy’s hard drive, including incriminating documents that fabricated links between Father Stan and the Maoist insurgency. The final incriminating document was planted on Father Stan’s computer on June 5, 2019, a week before the raid on him,” he added.

It was on the basis of these planted documents that Father Swamy was first arrested, in spite of experts raising serious doubts about the authenticity of the documents, Father Joseph Xavier added.

ADVERTISEMENT

It was on the basis of these planted documents that Father Swamy was first arrested, in spite of experts raising serious doubts about the authenticity of the documents, Father Xavier added.

Quoting Arsenal Consulting’s President, Mark Spencer, Father Xavier’s statement said: “The scale of what happened to Father Swamy and some of his co-defendants, in terms of the aggressive surveillance of their electronic devices which culminated in incriminating document deliveries over the course of years, is truly unprecedented.”

Father Xavier, in the statement, said Arsenal has effectively caught the attacker red-handed, based on remnants of their activity left behind in file system transactions, application execution data and other things. However, it has

Read more from America



Cardinal Gregory:
Pope Francis
makes Americans...
Kate Scanlon - OSV
News

“Cyber security firm Sentinel One has previously investigated the attackers and concluded that their ‘activity aligns sharply with Indian state interests,’” the statement added.

The statement further alleged that multiple findings link the suspected hackers to the Indian state.

Ucanews.com reported that Jesuit Father A. Santhanam, national convener of the National Lawyers Forum of Religious and Priests, said it had been proved that “Father Swamy was falsely implicated by the investigating agency by implanting fabricated evidence.”

He wondered if the federal government would expose its own agencies involved in the case, but said the world has the right to know who hacked the computer of Father Swamy.

“As a first remedy, the government and its agency should submit an unconditional apology for the elderly Jesuit’s death in custody,” Father Santhanam said.

He said the government also must take full responsibility and compensate for the loss of life, besides releasing all those accused and imprisoned in the Bhima-Koregaon case.

Bhima-Koregaon is a village in Maharashtra that has come to symbolize the bravery of the Dalits or former untouchables, who gather there to commemorate a 200-year-old battle victory on Jan. 1 every year.

In 2018, violence erupted at Bhima-Koregaon when some groups carrying saffron flags entered the scene and attacked the Dalits gathered for the annual victory celebration.

However, investigators alleged the violence was the handiwork of Maoist rebels and arrested 16 activists, alleging they were directly involved in the conspiracy.

“The major evidence on which the NIA was relying was the so-called incriminating evidence found in the computers and laptops, including that of Father Swamy. Now the forensic report has shattered this lie,” Father Santhanam said.

Father Swamy repeatedly denied any knowledge of the evidential material found inside his computer.

“Till his death, Father Swamy maintained he (was) innocent, but it's (too) late now,” Father Santhanam said while appealing to the federal government and its probe agency to drop all charges against the others accused in the case and compensate them for the hardships and harassments caused to them and their families.



More: [INTERNATIONAL](#) / [ASIA](#)

PROVIDE FEEDBACK ON THIS ARTICLE

Read more from America



**Cardinal Gregory:
Pope Francis
makes Americans...**
Kate Scanlon - OSV
News

MORE FROM AMERICA



Cardinal McElroy on ‘radical inclusion’ for L.G.B.T. people, women and others in the Catholic Church
Robert W. McElroy



‘Love’ gives a theatrical voice to the homeless with humor and heartbreak
Rhoda Feng



Retired priest barred from hearing confessions over support for law repealing the confessional seal
Gina Christian - OSV News



Students ‘no longer members’ of Catholic school after racist video
The Associated Press



U.S. bishops: Human composting is unacceptable for Catholic burials
Gina Christian - OSV News

CLASSIFIEDS
MARKETPLACE

Your source for jobs, books, retreats, and much more.

Read more from America



Cardinal Gregory: Pope Francis makes Americans...
Kate Scanlon - OSV News

Retreat Houses, Retreats

Parish Catechetical Leader – Director of Religious Education

Jobs

Wake Up With Purpose!: What I’ve Learned in My First Hundred Years

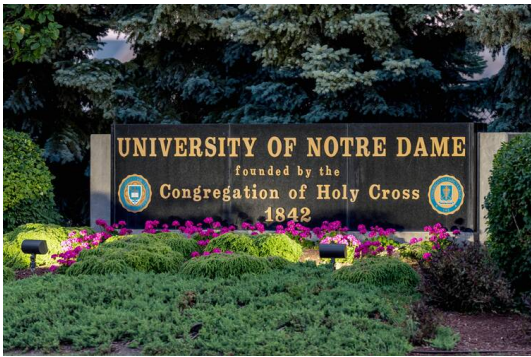
Books, Harper Horizon

Magis Theatre Company’s Logos Project production of *mark – a solo performance of the Gospel of Mark

Theater / Arts

[See all Classifieds](#)

WHAT TO READ NEXT



Bishop Rhoades: ‘Reproductive justice’ lecture series with abortion doula a ‘scandal,’ ‘unworthy’ of Notre Dame University

The decision “to provide an unanswered activist’s case that abortion is a tool of justice for the marginalized,” Bishop Kevin Rhoades wrote, “is a grave mistake in judgment that creates scandal.”

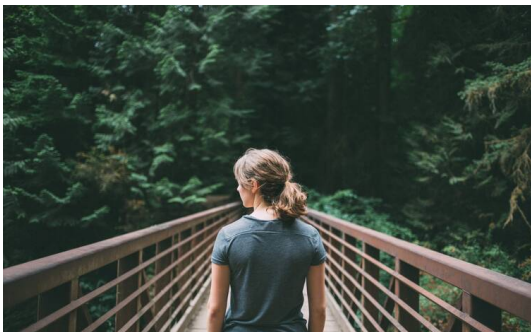
Kate Scanlon - OSV News March 23, 2023



Jesuit sexual abuse expert discusses the Marko Rupnik case, the Society of Jesus and the state of the abuse crisis

“The Society of Jesus is a mixed reality as the whole church is,” Father Zollner said, when asked about the lack of transparency in the Father Rupnik case. “We are not better at this. And it has been proven now, in the eyes of everybody, again.”

Paulina Guzik - OSV News March 6, 2023



God wants women to survive and thrive. Do we?

A Reflection for Monday of the Fifth Week of Lent, by Cecilia González-Andrieu

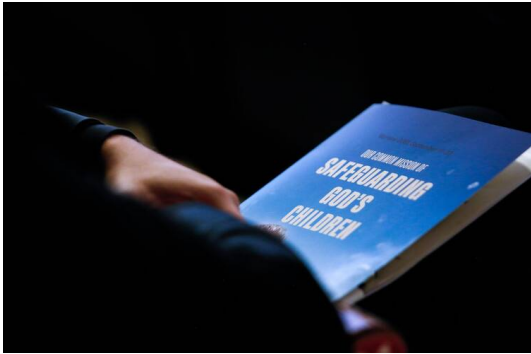
Cecilia González-Andrieu March 27, 2023

Read more from America



Cardinal Gregory: Pope Francis makes Americans...

Kate Scanlon - OSV News



We don't know enough about the causes of clergy sexual abuse. One Jesuit initiative is beginning to change that.

Fordham University's Taking Responsibility initiative released its final report on Feb. 9, calling for both clergy and lay members of Jesuit institutions to face "entangled responsibilities" around the abuse crisis.

Bradford E. Hinze March 23, 2023



A farewell and thank you to the New York Times Covid-19 tracker

In a time when we felt isolated, afraid and increasingly divided, The Times gave us a means to better understand what was happening and to stay connected with one another.

Jim McDermott March 27, 2023

Read more from America



Cardinal Gregory: Pope Francis makes Americans...
Kate Scanlon - OSV
News

Internal Exhibit E



X-SCITECH

Viruses Frame PC Owners for Child Porn

NOVEMBER 9, 2009 / 12:49 PM / CBS/AP

Of all the sinister things that Internet viruses do, this might be the worst: They can make you an unsuspecting collector of child pornography.

Heinous pictures and videos can be deposited on computers by viruses - the malicious programs better known for swiping your credit card numbers. In this twist, it's your reputation that's stolen.

Pedophiles can exploit virus-infected PCs to remotely store and view their stash without fear they'll get caught. Pranksters or someone trying to frame you can tap viruses to make it appear that you surf illegal Web sites.

Whatever the motivation, you get child porn on your computer - and might not realize it until police knock at your door.

An Associated Press investigation found cases in which innocent people have been branded as pedophiles after their co-workers or loved ones stumbled upon child porn placed on a PC through a virus. It can cost victims hundreds of thousands of dollars to prove their innocence.



Their situations are complicated by the fact that actual pedophiles often blame viruses - a defense rightfully viewed with skepticism by law enforcement.

"It's an example of the old 'dog ate my homework' excuse," says Phil Malone, director of the Cyberlaw Clinic at Harvard's Berkman Center for Internet & Society. "The problem is, sometimes the dog does eat your homework."

The AP's investigation included interviewing people who had been found with child porn on their computers. The AP reviewed court records and spoke to prosecutors, police and computer examiners.

One case involved Michael Fiola, a former investigator with the Massachusetts agency that oversees workers' compensation.

In 2007, Fiola's bosses became suspicious after the Internet bill for his state-issued laptop showed that he used 4½ times more data than his colleagues. A technician found child porn in the PC folder that stores images viewed online.

Fiola was fired and charged with possession of child pornography, which carries up to five years in prison. He endured death threats, his car tires were slashed and he was shunned by friends.

Fiola and his wife fought the case, spending \$250,000 on legal fees. They liquidated their savings, took a second mortgage and sold their car.

An inspection for his defense revealed the laptop was severely infected. It was programmed to visit as many as 40 child porn sites per minute - an inhuman feat. While Fiola and his wife were out to dinner one night, someone logged on to the computer and porn flowed in for an hour and a half.

Prosecutors performed another test and confirmed the defense findings. The charge was dropped - 11 months after it was filed.

The Fiolas say they have health problems from the stress of the case. They say they've talked to dozens of lawyers but can't get one to sue the state, because of a cap on the amount they can recover.

"It ruined my life, my wife's life and my family's life," he says.

The **Massachusetts attorney general's office**, which charged Fiola, declined interview requests.

At any moment, about 20 million of the estimated 1 billion Internet-connected PCs worldwide are infected with viruses that could give hackers full control, according to security software maker F-Secure

Corp. Computers often get infected when people open e-mail attachments from unknown sources or visit a malicious Web page.

Pedophiles can tap viruses in several ways. The simplest is to force someone else's computer to surf child porn sites, collecting images along the way. Or a computer can be made into a warehouse for pictures and videos that can be viewed remotely when the PC is online.

"They're kind of like locusts that descend on a cornfield: They eat up everything in sight and they move on to the next cornfield," says Eric Goldman, academic director of the **High Tech Law Institute at Santa Clara University**. Goldman has represented Web companies that discovered child pornographers were abusing their legitimate services.

But pedophiles need not be involved: Child porn can land on a computer in a sick prank or an attempt to frame the PC's owner.

In the first publicly known cases of individuals being victimized, two men in the United Kingdom were cleared in 2003 after viruses were shown to have been responsible for the child porn on their PCs.

In one case, an infected e-mail or pop-up ad poisoned a defense contractor's PC and downloaded the offensive pictures.

In the other, a virus changed the home page on a man's Web browser to display child porn, a discovery made by his 7-year-old daughter. The man spent more than a week in jail and three months in a halfway house, and lost custody of his daughter.

Chris Watts, a computer examiner in Britain, says he helped clear a hotel manager whose co-workers found child porn on the PC they shared with him.

Watts found that while surfing the Internet for ways to play computer games without paying for them, the manager had visited a site for pirated software. It redirected visitors to child porn sites if they were inactive for a certain period.

In all these cases, the central evidence wasn't in dispute: Pornography was on a computer. But proving how it got there was difficult.

Tami Loehrs, who inspected Fiola's computer, recalls a case in Arizona in which a computer was so "extensively infected" that it would be "virtually impossible" to prove what an indictment alleged: that a 16-year-old who used the PC had uploaded child pornography to a Yahoo group.

Prosecutors dropped the charge and let the boy plead guilty to a separate crime that kept him out of jail, though they say they did it only because of his age and lack of a criminal record.

Many prosecutors say blaming a computer virus for child porn is a new version of an old ploy.

"We call it the SODDI defense: Some Other Dude Did It," says James Anderson, a federal prosecutor in Wyoming.

However, forensic examiners say it would be hard for a pedophile to get away with his crime by using a bogus virus defense.

"I personally would feel more comfortable investing my retirement in the lottery before trying to defend myself with that," says forensics specialist Jeff Fischbach.

Even careful child porn collectors tend to leave incriminating e-mails, DVDs or other clues. Virus defenses are no match for such evidence,

says Damon King, trial attorney for the U.S. Justice Department's **Child Exploitation and Obscenity Section**.

But while the virus defense does not appear to be letting real pedophiles out of trouble, there have been cases in which forensic examiners insist that legitimate claims did not get completely aired.

Loehrs points to Ned Solon of Casper, Wyo., who is serving six years for child porn found in a folder used by a file-sharing program on his computer.

Solon admits he used the program to download video games and adult porn - but not child porn. So what could explain that material?

Loehrs testified that Solon's antivirus software wasn't working properly and appeared to have shut off for long stretches, a sign of an infection. She found no evidence the five child porn videos on Solon's computer had been viewed or downloaded fully. The porn was in a folder the file-sharing program labeled as "incomplete" because the downloads were canceled or generated an error.

This defense was curtailed, however, when Loehrs ended her investigation in a dispute with the judge over her fees. Computer exams can cost tens of thousands of dollars. Defendants can ask the courts to pay, but sometimes judges balk at the price. Although Loehrs stopped working for Solon, she argues he is innocent.

"I don't think it was him, I really don't," Loehrs says. "There was too much evidence that it wasn't him."

The prosecution's forensics expert, Randy Huff, maintains that Solon's antivirus software was working properly. And he says he ran other antivirus programs on the computer and didn't find an infection - although security experts say antivirus scans frequently miss things.

"He actually had a very clean computer compared to some of the other cases I do," Huff says.

The jury took two hours to convict Solon.

"Everybody feels they're innocent in prison. Nobody believes me because that's what everybody says," says Solon, whose case is being appealed. "All I know is I did not do it. I never put the stuff on there. I never saw the stuff on there. I can only hope that someday the truth will come out."

But can it? It can be impossible to tell with certainty how a file got onto a PC.

"Computers are not to be trusted," says Jeremiah Grossman, founder of WhiteHat Security Inc. He describes it as "painfully simple" to get a computer to download something the owner doesn't want - whether it's a program that displays ads or one that stores illegal pictures.

It's possible, Grossman says, that more illicit material is waiting to be discovered.

"Just because it's there doesn't mean the person intended for it to be there - whatever it is, child porn included."

Internal Exhibit F

Clickjacking

197.7k views

App SecurityThreats

What is clickjacking

Clickjacking is an attack that tricks a user into clicking a webpage element which is invisible or disguised as another element. This can cause users to unwittingly download malware, visit malicious web pages, provide credentials or sensitive information, transfer money, or purchase products online.

Typically, clickjacking is performed by displaying an invisible page or HTML element, inside an iframe, on top of the page the user sees. The user believes they are clicking the visible page but in fact they are clicking an invisible element in the additional page transposed on top of it.

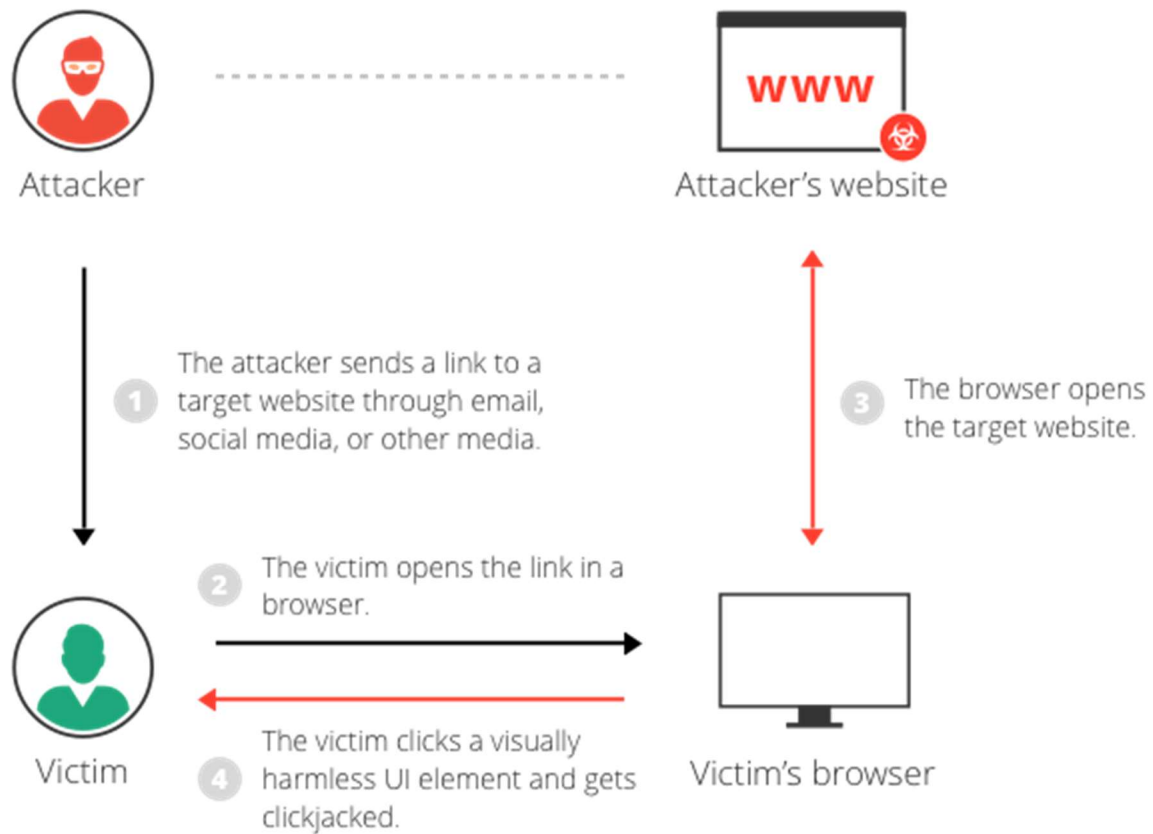
The invisible page could be a [malicious page](#), or a legitimate page the user did not intend to visit – for example, a page on the user's banking site that authorizes the transfer of money.

There are several variations of the clickjacking attack, such as:

- **Likejacking** – a technique in which the Facebook "Like" button is manipulated, causing users to "like" a page they actually did not intend to like.
- **Cursorjacking** – a UI redressing technique that changes the cursor for the position the user perceives to another position. Cursorjacking relies on vulnerabilities in Flash and the Firefox browser, which have now been fixed.

Clickjacking attack example

1. The attacker creates an attractive page which promises to give the user a free trip to Tahiti.
2. In the background the attacker checks if the user is logged into his banking site and if so, loads the screen that enables transfer of funds, using query parameters to insert the attacker's bank details into the form.
3. The bank transfer page is displayed in an invisible iframe above the free gift page, with the "Confirm Transfer" button exactly aligned over the "Receive Gift" button visible to the user.
4. The user visits the page and clicks the "Book My Free Trip" button.
5. In reality the user is clicking on the invisible iframe, and has clicked the "Confirm Transfer" button. Funds are transferred to the attacker.
6. The user is redirected to a page with information about the free gift (not knowing what happened in the background).



This example illustrates that, in a clickjacking attack, the malicious action (on the bank website, in this case) cannot be traced back to the [attacker](#) because the user performed it while being legitimately signed into their own account.

Clickjacking mitigation

There are two general ways to defend against clickjacking:

- **Client-side methods** – the most common is called Frame Busting. Client-side methods can be effective in some cases, but are considered not to be a best practice, because they can be easily bypassed.

- **Server-side methods** – the most common is X-Frame-Options. Server-side methods are recommended by security experts as an effective way to defend against clickjacking.

Mitigating clickjacking with X-Frame-Options response header

The X-Frame-Options response header is passed as part of the HTTP response of a web page, indicating whether or not a browser should be allowed to render a page inside a <FRAME> or <IFRAME> tag.

There are three values allowed for the X-Frame-Options header:

- **DENY** – does not allow any domain to display this page within a frame
- **SAMEORIGIN** – allows the current page to be displayed in a frame on another page, but only within the current domain
- **ALLOW-FROM URI** – allows the current page to be displayed in a frame, but only in a specific URI – for example *www.example.com/frame-page*

See how Imperva [Web Application Firewall can help you with clickjacking attacks](#).

[Request demo](#) [Learn more](#)

Using the SAMEORIGIN option to defend against clickjacking

X-Frame-Options allows content publishers to prevent their own content from being used in an invisible frame by attackers.

The DENY option is the most secure, preventing any use of the current page in a frame. More commonly, SAMEORIGIN is used, as it does enable the use of frames, but limits them to the current domain.

Limitations of X-Frame-Options

- To enable the SAMEORIGIN option across a website, the X-Frame-Options header needs to be returned as part of the HTTP response for each individual page (cannot be applied cross-site).
- X-Frame-Options does not support a whitelist of allowed domains, so it doesn't work with multi-domain sites that need to display framed content between them.
- Only one option can be used on a single page, so, for example, it is not possible for the same page to be displayed as a frame both on the current website and an external site.
- The ALLOW-FROM option is not supported by all browsers.
- X-Frame-Options is a deprecated option in most browsers.

Clickjacking test – Is your site vulnerable?

A basic way to test if your site is [vulnerable](#) to clickjacking is to create an HTML page and attempt to include a sensitive page from your website in an iframe. It is important to execute the test code on another web server, because this is the typical behavior in a clickjacking attack.

Use code like the following, provided as part of the [OWASP Testing Guide](#):

```
<html>

<head>

<title>Clickjack test page</title>

</head>

<body>

<p>Website is vulnerable to clickjacking!</p>
```



```
<iframe src="http://www.yoursite.com/sensitive-page" width="500"
height="500"></iframe>

</body>

</html>
```

View the HTML page in a browser and evaluate the page as follows:

- If the text "Website is vulnerable to clickjacking" appears and below it you see the content of your sensitive page, **the page is vulnerable to clickjacking**.
- If only the text "Website is vulnerable to clickjacking" appears, and you do not see the content of your sensitive page, the page is not vulnerable to the simplest form of clickjacking.

However, additional testing is needed to see which anti-clickjacking methods are used on the page, and whether they can be bypassed by attackers.

How Imperva helps mitigate clickjacking attack

To get to the point of clickjacking a site, the site will have to be compromised, something [Imperva WAF](#) prevents. You should also make sure your site resources are sending the proper X-Frame-Options HTTP headers, which would prevent some parts of your site from being framed in other pages or outside your domain.

Internal Exhibit G




7 Exercise Tips How to Stream 'Rabbit Hole' Roblox's AI Efforts 9 Household Items You're Not Cleaning Enough Better Sound on FaceTime Calls

CNET Your guide to a better future

Tech > Services & Software

FBI won't reveal hack, so child porn evidence tossed

The FBI's hacking method, which allowed agents to track the defendant as he allegedly perused the so-called Dark Web, leads a federal judge to exclude the very evidence that could lead to his conviction.

 **Laura Hautala** May 25, 2016 6:28 p.m. PT 3 min read 



WASHINGTON, DC - AUGUST 20: The exterior of the J. Edgar Hoover Building, which is the headquarters of the FBI is seen on Thursday August 20, 2015 in Washington, DC. The agency is looking for a new location for their headquarters. (Photo by Matt McClain/The Washington Post via Getty Images)
Matt McClain, The Washington Post/Getty Images

Evidence in a child pornography trial has been thrown out because the FBI won't reveal how it tracked the defendant.

Want CNET to notify you of price drops and the latest stories? No, thank you

The FBI says the hacking method, referred to as a Network Investigation Technique, or NIT, allowed the bureau to track Jay Michaud after he visited a hidden website on the so-called Dark Web, leading to charges of possessing child pornography. Defense attorneys say a government explanation could show that the method yielded unreliable information.

The case is part of a growing debate over government hacking in criminal cases. Michaud is one of several people facing charges after the bureau used the hacking method to infiltrate the hidden child pornography website and identify the computers of those who visited it. A handful of those cases have seen evidence tossed out as well. In addition to concerns over the reliability of the hack raised by Michaud's attorneys, judges have raised concerns over warrants that allow the government to target a computer even when its location is unknown.

As the resulting cases have unfolded, the US Senate is considering a change to federal judicial rules that would let judges sign warrants to permit the government to target computers outside their jurisdiction when their locations are unknown.

In the case of Michaud, who was a middle school teacher in Vancouver, Wash., the technique led police to obtain a search warrant last year for his home, where they allegedly found a cell phone and two thumb drives containing child pornography. That evidence is no longer part of the case.

"Evidence of the NIT, the search warrant issued based on the NIT, and the fruits of that warrant should be excluded and should not be offered in evidence at trial," Judge Robert J. Bryan of the US District Court of the Western District of Washington wrote in his opinion Wednesday, issued after a hearing.

Michaud allegedly visited the child pornography site through the Tor browser, a tool that lets Internet users disguise their locations and visit hidden areas of the Web.

His attorneys argued that he had a right to know exactly how the government carried out the alleged hack, "given the sophistication of the FBI's surveillance technology and the evidence that it has misled the courts in other cases about that technology."

The brief cited a report from the Associated Press about cases in which child pornography was found stashed on the hacked com



Want CNET to notify you of price drops and the latest stories?

No, thank you

Accept

Advertisement



Advertisement

Colin Fieman, a federal public defender representing Michaud, did not respond to a request for comment.

The judge had already ordered the government to turn over its code, but the US Attorney asked him to reconsider. After pointing out the files containing alleged child pornography were found on the defendant's thumb drives and cell phone, the US Attorney's brief said, "any concern about corruption or other errors that might cast doubt on the accuracy of the information obtained through the NIT...can be addressed by review of the information that was actually collected."

The US Department of Justice did not respond to a request for comment on the case.

While Bryan ruled Wednesday to exclude evidence from the trial, he also wrote that the case shouldn't be dismissed.



Advertisement



Internal Exhibit H



PUBLICATIONS

Keyloggers: How they work and how to detect them (Part 1)

29 MAR 2007 ⌚ 14 minute read



Table of Contents

[Keyloggers: Implementing keyloggers in Windows. Part Two](#)

In February 2005, Joe Lopez, a businessman from Florida, filed a [suit](#) against Bank of America after unknown hackers stole \$90,000 from his Bank of America account. The money had been transferred to Latvia.

An investigation showed that Mr. Lopez's computer was infected with a malicious program, Backdoor.Coreflood, which records every keystroke and sends this information to malicious users via the Internet. This is how the hackers got hold of Joe Lopez's user name and password, since Mr. Lopez often used the Internet to manage his Bank of America account.

Kaspersky Glossary

Helps explain infosec in lay terms

Visit

However the court did not rule in favor of the plaintiff, saying that Mr. Lopez had neglected to take basic precautions when managing his bank account on the Internet: a signature for the malicious code that was found on his system had been added to nearly all antivirus product databases back in 2003.

Joe Lopez's losses were caused by a combination of overall carelessness and an ordinary keylogging program.

About Keyloggers

The term 'keylogger' itself is neutral, and the word describes the program's function. Most sources define a keylogger as a software program designed to secretly monitor and log all keystrokes. This definition is not altogether correct, since a keylogger doesn't have to be software – it can also be a device. Keylogging devices are much rarer than keylogging software, but it is important to keep their existence in mind when thinking about information security.

Kaspersky Encyclopedia

of threats and attack vectors

Visit

Legitimate programs may have a keylogging function which can be used to call certain program functions using "hotkeys," or to toggle between keyboard layouts (e.g. Keyboard Ninja). There is a lot of legitimate software which is designed to allow administrators to track what employees do throughout the day, or to allow users to track the activity of third parties on their computers. However, the ethical boundary between justified monitoring and espionage is a fine line. Legitimate software is often used deliberately to steal confidential user information such as passwords.

Most modern keyloggers are considered to be legitimate software or hardware and are sold on the open market. Developers and vendors offer a long list of cases in which it would be legal and appropriate to use keyloggers, including:

Parental control: parents can track what their children do on the Internet, and can opt to be notified if there are any attempts to access websites containing adult or otherwise inappropriate content;

Jealous spouses or partners can use a keylogger to track the actions of their better half on the Internet if they suspect them of “virtual cheating”;

Company security: tracking the use of computers for non-work-related purposes, or the use of workstations after hours;

Company security: using keyloggers to track the input of key words and phrases associated with commercial information which could damage the company (materially or otherwise) if disclosed;

Other security (e.g. law enforcement): using keylogger records to analyze and track incidents linked to the use of personal computers;

Other reasons.

However, the justifications listed above are more subjective than objective; the situations can all be resolved using other methods. Additionally, **any** legitimate keylogging program can still be used with malicious or criminal intent. Today, keyloggers are mainly used to steal user data relating to various online payment systems, and virus writers are constantly writing new keylogger Trojans for this very purpose.

Furthermore, many keyloggers hide themselves in the system (i.e. they have rootkit functionality), which makes them fully-fledged Trojan programs.

As such programs are extensively used by cyber criminals, detecting them is a priority for antivirus companies. Kaspersky Lab's malware classification system has a dedicated category for malicious programs **with keylogging functionality**: Trojan-Spy. Trojan-Spy programs, as the name suggests, track user activity, save the information to the user's hard disk and then forward it to the author or 'master' of the Trojan. The information collected includes keystrokes and screen-shots, used in the theft of banking data to support online fraud.

Why keyloggers are a threat

Unlike other types of malicious program, keyloggers present no threat to the system itself. Nevertheless, they can pose a serious threat to users, as they can be used to intercept passwords and other confidential information entered via the keyboard. As a result, cyber criminals can get PIN codes and account numbers for e-payment systems, passwords to online gaming accounts, email addresses, user names, email passwords etc.

Once a cyber criminal has got hold of confidential user data, s/he can easily transfer money from the user's account or access the user's online gaming account. Unfortunately access to confidential data can sometimes have consequences which are far more serious than an individual's loss of a few dollars. Keyloggers can be used as tools in both industrial and political espionage, accessing data which may include proprietary commercial information and classified government material which could compromise the security of commercial and state-owned organizations (for example, by stealing private encryption keys).

Keyloggers, phishing and social engineering (see '**Computers, Networks and Theft**') are currently the main methods being used in cyber fraud. Users who are aware of security issues can easily protect themselves against phishing by ignoring phishing emails and by not entering any personal information on suspicious websites. It is more difficult, however, for users to combat keyloggers; the only possible method is to use an appropriate security solution, as it's usually impossible for a user to tell that a keylogger has been installed on his/ her machine.

According to Cristine Hoepers, the manager of Brazil's Computer Emergency Response Team, which works under the aegis of the country's Internet Steering Committee, keyloggers have pushed phishing out of first place as the most-used method in the theft of confidential information. What's more, keyloggers are becoming more sophisticated – they track websites visited by the user and only log keystrokes entered on websites of particular interest to the cyber criminal.

In recent years, we have seen a considerable increase in the number of different kinds of malicious programs which have keylogging functionality. No Internet user is immune to cyber criminals, no matter where in the world s/he is located and no matter what organization s/he works for.

How cyber criminals use keyloggers

One of the most publicized keylogging incidents recently was the **theft** of over \$1million from client accounts at the major Scandinavian bank Nordea. In August 2006 Nordea clients started to receive emails, allegedly from the bank, suggesting that they install an antispam product, which was supposedly attached to the message. When a user opened the file and downloaded it to his/ her computer, the machine would be infected with a well known Trojan called Haxdoor. This would be activated when the victim registered at Nordea's online service, and the Trojan would display an error notification with a request to re-enter the registration information. The keylogger incorporated in the Trojan would record data entered by the bank's clients, and later send this data to the cyber criminals' server. This was how cyber criminals were able to access client accounts, and transfer money from them. According to Haxdoor's author, the Trojan has also been used in attacks against Australian banks and many others.

On January 24, 2004 the notorious Mydoom worm caused a **major epidemic**. MyDoom broke the record previously set by Sobig, provoking the largest epidemic in Internet history to date. The worm used social engineering methods and organized a DoS attack on www.sco.com; the site was either unreachable or unstable for several months as a consequence. The worm left a Trojan on infected computers which was subsequently used to infect the victim machines with new modifications of the worm. The fact that MyDoom had a keylogging function to harvest credit card numbers was not widely publicized in the media.

In early 2005 the London police **prevented** a serious attempt to steal banking data. After attacking a banking system, the cyber criminals had planned to steal \$423 million from Sumitomo Mitsui's London-based offices. The main component of the Trojan used, which was created by the 32-year-old Yeron Bolondi, was a keylogger that allowed the criminals to track all the keystrokes entered when victims used the bank's client interface.

In May 2005 a **married couple** was arrested in London who were charged with developing malicious programs that were used by some Israeli companies in **industrial espionage**. The scale of the espionage was shocking: the companies named by the Israeli authorities in investigative reports included cellular providers like Cellcom and Pelephone, and satellite television provider YES. According to reports, the Trojan was used to access information relating to the PR agency Rani Rahav, whose clients included Partner Communications (Israel's second leading cellular services provider) and the HOT cable television group. The Mayer company, which imports Volvo and Honda cars to Israel, was suspected of committing industrial espionage against Champion Motors, which imports Audi and Volkswagen cars to the country. Ruth Brier-Haephraati, who sold the keylogging Trojan that her husband Michael Haephraati created, was sentenced to four years in jail, and Michael received a two-year sentence.

In February 2006, the Brazilian police arrested 55 people involved in spreading malicious programs which were used to steal user information and passwords to banking systems. The keyloggers were activated when the users visited their banks' websites, and secretly tracked and subsequently sent all data entered on these pages to cyber criminals. The total amount of money stolen from 200 client accounts at six of the country's banks totaled \$4.7million.

At approximately the same time, a similar criminal grouping made up of young (20 – 30 year old) Russians and Ukrainians was arrested. In late 2004, the group began sending banking clients in France and a number of other countries email messages that contained a malicious program – namely, a keylogger. Furthermore, these spy programs were placed on specially created websites; users were lured to these sites using classic social engineering methods. In the same way as in the cases described above, the program was activated when users visited their banks' websites, and the keylogger harvested all the information entered by the user and sent it to the cyber criminals. In the course of eleven months over one million dollars was stolen.

There are many more examples of cyber criminals using keyloggers – most financial cybercrime is committed using keyloggers, since these programs are the most comprehensive and reliable tool for tracking electronic information.

Increased use of keyloggers by cyber criminals

The fact that cyber criminals choose to use keyloggers time and again is confirmed by IT security companies.

One of VeriSign's recent reports notes that in recent years, the company has seen a rapid growth in the number of malicious programs that have keylogging functionality.

Source: iDefense, a VeriSign Company

One report issued by Symantec shows that almost 50% of malicious programs detected by the company's analysts during the past year do not pose a direct threat to computers, but instead are used by cyber criminals to harvest personal user data.

According to research conducted by John Bambenek, an analyst at the SANS Institute, approximately 10 million computers in the US alone are currently infected with a malicious program which has a keylogging function. Using these figures, together with the total number of American users of e-payment systems, possible losses are estimated to be \$24.3 million.

Kaspersky Lab is constantly detecting new malicious programs which have a keylogging function. One of the first virus alerts on securelist.com, Kaspersky Lab's dedicated malware information site, was published on 15th June 2001. The warning related to TROJ_LATINUS.SVR, a Trojan with a keylogging function. Since then, there has been a steady

stream of new keyloggers and new modifications. Kaspersky antivirus database currently contain records for more than 300 families of keyloggers. This number does not include keyloggers that are part of complex threats (i.e. in which the spy component provides additional functionality).

Most modern malicious programs are hybrids which implement many different technologies. Due to this, any category of malicious program may include programs with keylogger (sub)functionality. The number of spy programs detected by Kaspersky Lab each month is on the increase, and most of these programs use keylogging technology.

Keylogger construction

The main idea behind keyloggers is to get in between any two links in the chain of events between when a key is pressed and when information about that keystroke is displayed on the monitor. This can be achieved using video surveillance, a hardware bug in the keyboard, wiring or the computer itself, intercepting input/ output, substituting the keyboard driver, the filter driver in the keyboard stack, intercepting kernel functions by any means possible (substituting addresses in system tables, splicing function code, etc.), intercepting DLL functions in user mode, and, finally, requesting information from the keyboard using standard documented methods.

Experience shows that the more complex the approach, the less likely it is to be used in common Trojan programs and the more likely it is to be used in specially designed Trojan programs which are designed to steal financial data from a specific company.

Keyloggers can be divided into two categories: keylogging devices and keylogging software. Keyloggers which fall into the first category are usually small devices that can be fixed to the keyboard, or placed within a cable or the computer itself. The keylogging software category is made up of dedicated programs designed to track and log keystrokes.

The most common methods used to construct keylogging software are as follows:

- a system hook which intercepts notification that a key has been pressed (installed using WinAPI SetWindowsHook for messages sent by the window procedure. It is most often written in C);

- a cyclical information keyboard request from the keyboard (using WinAPI Get(Async)KeyState or GetKeyboardState – most often written in Visual Basic, sometimes in Borland Delphi);

- using a filter driver (requires specialized knowledge and is written in C).

We will provide a detailed explanation of the different ways keyloggers are constructed in the second half of this article (to be published in the near future). But first, here are some statistics.

A rough breakdown of the different types of keyloggers is shown in the pie chart below:

Recently, keyloggers that disguise their files to keep them from being found manually or by an antivirus program have become more numerous. These stealth techniques are called rootkit technologies. There are two main rootkit technologies used by keyloggers:

- masking in user mode;
- masking in kernel mode.

A rough breakdown of the techniques used by keyloggers to mask their activity is shown in the pie chart below:

How keyloggers spread

Keyloggers spread in much the same way that other malicious programs spread. Excluding cases where keyloggers are purchased and installed by a jealous spouse or partner, and the use of keyloggers by security services, keyloggers are mostly spread using the following methods):

- a keylogger can be installed when a user opens a file attached to an email;
- a keylogger can be installed when a file is launched from an open-access directory on a P2P network;
- a keylogger can be installed via a web page script which exploits a browser vulnerability. The program will automatically be launched when a user visits a infected site;
- a keylogger can be installed by another malicious program already present on the victim machine, if the program is capable of downloading and installing other malware to the system.

How to protect yourself from keyloggers

Most antivirus companies have already added known keyloggers to their databases, making protecting against keyloggers no different from protecting against other types of malicious program: install an antivirus product and keep its database up to date. However, since most antivirus products classify keyloggers as *potentially malicious*, or *potentially undesirable programs*, users should ensure that their antivirus product will, with default settings, detect this type of malware. If not, then the product should be configured accordingly, to ensure protection against most common keyloggers.

Let's take a closer look at the methods that can be used to protect against unknown keyloggers or a keylogger designed to target a specific system.

Since the chief purpose of keyloggers is to get confidential data (bank card numbers, passwords, etc.), the most logical ways to protect against unknown keyloggers are as follows:

- 1 using one-time passwords or two-step authentication,
- 2 using a system with proactive protection designed to detect keylogging software,
- 3 using a virtual keyboard.

Using a one-time password can help minimize losses if the password you enter is intercepted, as the password generated can be used one time only, and the period of time during which the password can be used is limited. Even if a one-time password is intercepted, a cyber criminal will not be able to use it in order to obtain access to confidential information.

In order to get one-time passwords, you can use a special device such as:

- 1 a USB key (such as [Aladdin eToken NG OTP](#) (page in Russian)):
- 2 a 'calculator' (such as [RSA SecurID 900 Signing Token](#)):

In order to generate one-time passwords, you can also use mobile phone text messaging systems that are registered with the banking system and receive a PIN-code as a reply. The PIN is then used together with the personal code for authentication.

If either of the above devices is used to generate passwords, the procedure is as described below:

- 1 the user connects to the Internet and opens a dialogue box where personal data should be entered;
- 2 the user then presses a button on the device to generate a one-time password, and a password will appear on the device's LCD display for 15 seconds;
- 3 the user enters his user name, personal PIN code and the generated one-time password in the dialogue box (usually the PIN code and the key are entered one after the other in a single pass code field);
- 4 the codes that are entered are verified by the server, and a decision is made whether or not the user may access confidential data.

When using a calculator device to generate a password, the user will enter his PIN code on the device 'keyboard' and press the ">" button.

One-time password generators are widely used by banking systems in Europe, Asia, the US and Australia. For example, Lloyds TSB, a leading bank, decided to **use** password generators back in November 2005.

In this case, however, the company has to spend a considerable amount of money as it had to acquire and distribute password generators to its clients, and develop/ purchase the accompanying software.

A more cost efficient solution is proactive protection on the client side, which can warn a user if an attempt is made to install or activate keylogging software.

Proactive protection against keyloggers in Kaspersky Internet Security

The main drawback of this method is that the user is actively involved and has to decide what action should be taken. If a user is not very technically experienced, s/he might make the wrong decision, resulting in a keylogger being allowed to bypass the antivirus solution. However, if developers minimize user involvement, then keyloggers will be able to evade detection due to an insufficiently rigorous security policy. However, if settings are too stringent, then other, useful programs which contain legitimate keylogging functions might also be blocked.

The final method which can be used to protect against both keylogging software and hardware is using a **virtual keyboard**. A virtual keyboard is a program that shows a keyboard on the screen, and the keys can be 'pressed' by using a mouse.

The idea of an on-screen keyboard is nothing new – the Windows operating system has a built-in on-screen keyboard that can be launched as follows: Start > Programs > Accessories > Accessibility > On-Screen Keyboard.

An example of the Windows on-screen keyboard

However, on-screen keyboards aren't a very popular method of outsmarting keyloggers. They were not designed to protect against cyber threats, but as an accessibility tool for disabled users. Information entered using an on-screen keyboard can easily be intercepted by a malicious program. In order to be used to protect against keyloggers, on-screen keyboards have to be specially designed in order to ensure that information entered or transmitted via the on-screen keyboard cannot be intercepted.

Conclusions

This article has provided an overview of how keyloggers – both keylogging software and hardware – function and are used.

Even though keylogger developers market their products as legitimate software, most keyloggers can be used to steal personal user data and in political and industrial espionage.

At present, keyloggers – together with phishing and social engineering methods – are one of the most commonly used methods of cyber fraud.

IT security companies have recorded a steady increase in the number of malicious programs that have keylogging functionality.

Reports show that there is an increased tendency to use rootkit technologies in keylogging software, to help the keylogger evade manual detection and detection by antivirus solutions.

Only dedicated protection can detect that a keylogger is being used for spy purposes.

The following measures can be taken to protect against keyloggers:

- use a standard antivirus that can be adjusted to detect potentially malicious software (default settings for many products);
- proactive protection will protect the system against new modifications of existing keyloggers;
- use a virtual keyboard or a system to generate one-time passwords to protect against keylogging software and hardware.

Keyloggers: Implementing keyloggers in Windows. Part Two

ANTIVIRUS TECHNOLOGIES

KEYLOGGERS

MALWARE TECHNOLOGIES

Authors